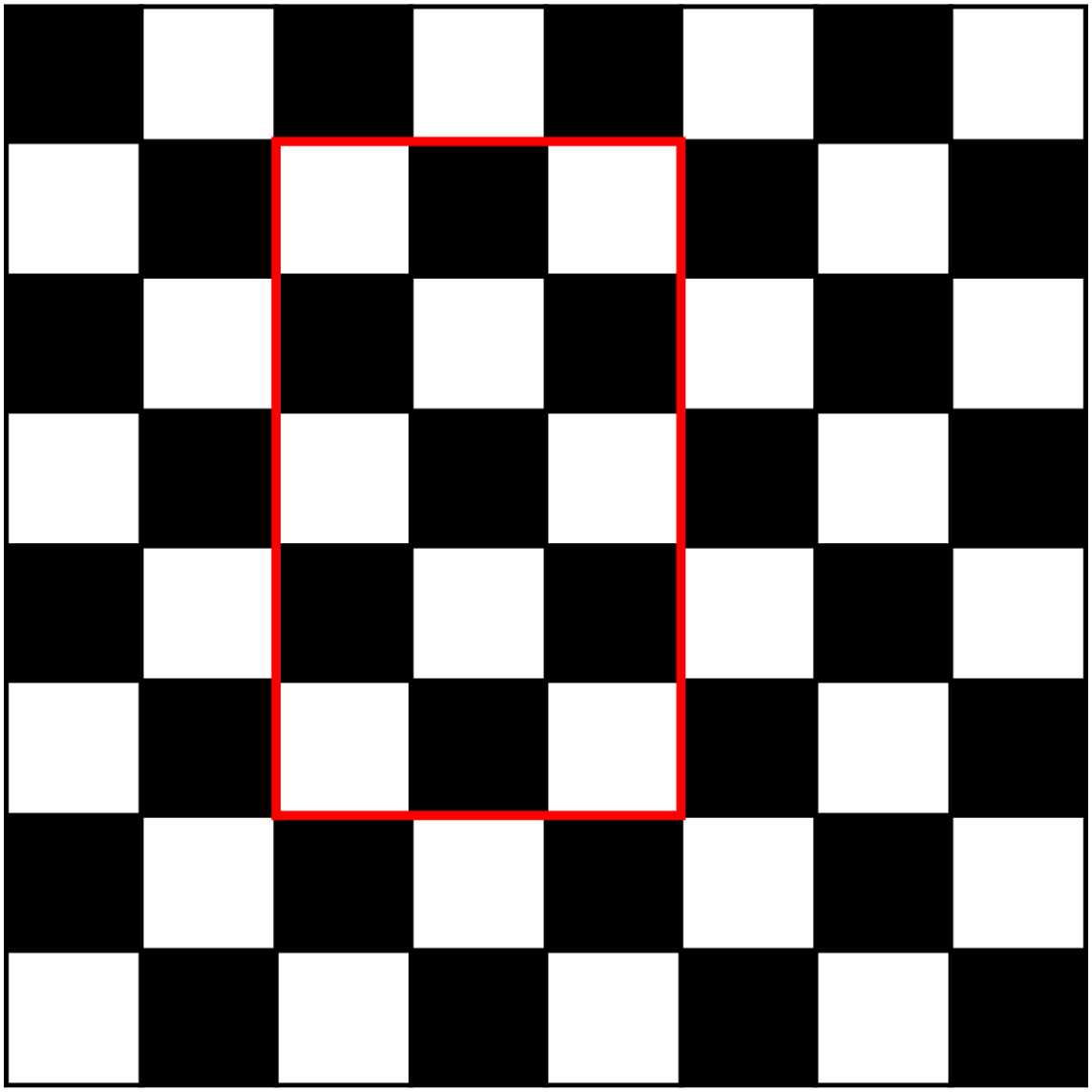
ΔΙΑΚΡΙΤΑ ΜΑΘΗΜΑΤΙΚΑ



Μιχάλης Κολουντζάκης & Χρήστος Παπαχριστόδουλος

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών

Πανεπιστήμιο Κρήτης

Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα
www.kallipos.gr

HEALLINK
Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΜΙΧΑΛΗΣ ΚΟΛΟΥΝΤΖΑΚΗΣ

ΧΡΗΣΤΟΣ ΠΑΠΑΧΡΙΣΤΟΔΟΥΛΟΣ

Διακριτά Μαθηματικά


Ελληνικά Ακαδημαϊκά Ηλεκτρονικά
Συγγράμματα και Βοηθήματα
www.kallipos.gr

Διακριτά Μαθηματικά

Συγγραφή

Μιχάλης Κολουντζάκης

Χρήστος Παπαχριστόδουλος

Κριτικός αναγνώστης

Μιχαήλ Λουλάκης

ISBN: 978-960-603-361-2

ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ

Εθνικό Μετσόβιο Πολυτεχνείο

Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

www.kallipos.gr

Περιεχόμενα

Ακρωνύμια

Οι παρακάτω όροι υπάρχουν και στο ευρετήριο στο τέλος του βιβλίου.

Συντομογραφία	Επεξήγηση
ASCII	American Standard Code For Information Interchange
CFG	Context Free Grammar
CFL	Context Free Language
DFA	Deterministic Finite Automaton
NFA	Non-deterministic Finite Automata
NP	Non-deterministic Polynomial Time
PDA	Push Down Automaton
ΣΞΑ	Σύστημα Ξένων Αντιπροσώπων
TM	Τυχαία Μεταβλητή

Πρόλογος

Η τελευταία έκδοση του βιβλίου αυτού θα βρίσκεται στη θέση

http://mk.eigen-space.org/discretebook

Στο βιβλίο αυτό υπάρχουν οι βασικές γνώσεις Διακριτών Μαθηματικών, Διακριτής Πιθανότητας και Τυπικών Γλωσσών που μπορεί κανείς να δει να διδάσκονται σε ένα τμήμα πληροφορικής ή ηλεκτρολόγων μηχανικών, αλλά, τώρα τελευταία, και σε τμήματα μαθηματικών ή εφαρμοσμένων μαθηματικών.

Για να μπορεί κανείς να δει το βιβλίο αυτό σωστά πρέπει να χρησιμοποιήσει υπολογιστή συνδεδεμένο στο διαδίκτυο. Υπάρχουν μέσα στο PDF σύνδεσμοι (links) προς

- video τα οποία βρίσκονται στο youtube,
- online ερωτήσεις τις οποίες ο αναγνώστης απαντάει (αριθμητική απάντηση) και το σύστημα απαντάει αν είναι σωστή η απάντησή του ή όχι.

Ανάλογα με το πρόγραμμα που χρησιμοποιεί κανείς για να δει το PDF μπορεί οι σύνδεσμοι να ανοίγουν στον browser με ένα απλό κλικ ή όχι. Στη δεύτερη περίπτωση κάντε copy τον σύνδεσμο μέσα από το PDF και κάντε το paste στη γραμμή διευθύσεων του browser για να ανοίξει.

Σύμβολα που χρησιμοποιούνται:

 Υπόδειξη για τη λύση μιας άσκησης.

 Online video. Στα video αυτά (που βρίσκονται στο youtube) παρουσιάζονται οι βασικές έννοιες και παραδείγματα.

 Κώδικας σε python. Οι ασκήσεις αυτές θα μπορούν να αποφεύγονται αν οι φοιτητές δεν έχουν την προαπαιτούμενη γνώση στον προγραμματισμό ή αν έτσι κρίνει ο διδάσκων.

Κεφάλαιο 1

Βασικές έννοιες από τη Θεωρία Συνόλων και τον Προτασιακό Λογισμό

Κύριες βιβλιογραφικές αναφορές για αυτό το Κεφάλαιο είναι οι Kamke 1950, Halmos 1960 και C. L. Liu and C. Liu 1985.

1.1 Εισαγωγή

Η σύγχρονη θεωρία συνόλων θεμελιώθηκε από τους Cantor και Dedekind την δεκαετία του 1870. Στις αρχές του 20ου αιώνα έχουν εισαχθεί διάφορα συστήματα αξιωμάτων για την θεμελίωση της θεωρίας συνόλων,με κυριότερο το σύστημα αξιωμάτων των Zermelo–Frankel. Στο κεφάλαιο αυτό δε θα ασχοληθούμε με τέτοια «αξιωματικά» θέματα. Σκοπός είναι να εισαγάγουμε τις βασικές έννοιες και θεωρήματα που θα χρειαστούμε σε αύτο το βιβλίο, τα οποία γενικότερα είναι εκείνα που χρειάζεται να γνωρίζουν οι φοιτητές θετικών επιστημών.

1.2 Σύνολα

Ένα σύνολο είναι μία συλλογή από αντικείμενα που ονομάζονται μέλη ή στοιχεία ή σημεία του συνόλου. Τα σύνολα τα συμβολίζουμε συνήθως με κεφαλαία γράμματα. Για να δηλώσουμε ότι ένα αντικείμενο p είναι μέλος ενός συνόλου A, γράφουμε:

$$p \in A$$

(διαβάζεται: το p ανήκει στο A). Για να δηλώσουμε ότι δεν ανήκει στο A γράφουμε:

$$p \notin A$$

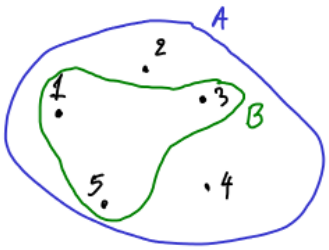
(διαβάζεται: το p δεν ανήκει στο A).

Ορισμός 1.1
(Κενό Σύνολο) *Το σύνολο που δεν έχει μέλη, κάτι σα μία άδεια τσάντα, ονομάζεται* κενό σύνολο *και συμβολίζεται με το σύμβολο* $\emptyset$.

Παράσταση Συνόλου: Για να περιγράψουμε ένα σύνολο υπάρχουν διάφοροι τρόποι:

1. Να καταγράψουμε μία λίστα με τα στοιχεία του μέσα σε άγγιστρα, π.χ. το σύνολο με μέλη τα αντικείμενα a, b, c γράφεται
$$\{a, b, c\}.$$
Το σύνολο με μόνο στοιχείο ένα αντικείμενο a γράφεται $\{a\}$ και λέγεται *μονοσύνολο*.

2. Να τα παραστήσουμε σχηματικά με ένα διάγραμμα Venn. Π.χ., μπορούμε να παραστήσουμε σχηματικά τα δύο σύνολα
$$A = \{1, 2, 3, 4, 5\},$$
και
$$B = \{1, 3, 5\},$$
με το παρακάτω Σχήμα 1.1.

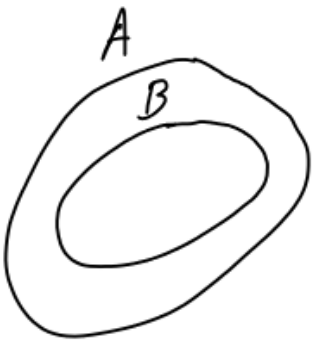


Σχήμα 1.1: Τα δύο σύνολα A και B σε διάγραμμα Venn

3. Συχνότερα όμως για να ορίσουμε ένα σύνολο δηλώνουμε μια ιδιότητα (πρόταση) $P(x)$ που αφορά αντικείμενα, πραγματικά ή ιδεατά, (όπως π.χ. είναι οι αριθμοί), η επαλήθευση της οποίας από ένα αντικείμενο x είναι αναγκαία και ικανή συνθήκη για να ανήκει το αντικείμενο αύτο στο σύνολο. Γράφουμε
$$\{x : P(x)\},$$
για να δηλώσουμε το σύνολο που έχει σαν μέλη τα αντικείμενα x ικανοποιούν την ιδιότητα $P(x)$.
Επίσης συνήθως αντί να γράφουμε:
$$\{x : \ x \in S \ \& \ P(x)\},$$
γράφουμε:
$$\{x \in S : \ P(x)\}.$$

Παράδειγμα 1.1
Το σύνολο
$$\{x : \ x \in \mathbb{Z} \ \& \ x^2 < 100\}$$
περιέχει εκείνους τους ακεραίους που έχουν τετράγωνο μικρότερο από 100.
Το ίδιο σύνολο πιο σύντομα γράφεται
$$\{x \in \mathbb{Z} : x^2 < 100\}.$$
Πρόκειται βεβαίως για ένα διαφορετικό τρόπο γραφής του συνόλου (βλέπουμε εδώ μια νέα συντομογραφία)
$$\{-9, -8, \ldots, 8, 9\}$$
που περιέχει όλους τους ακεραίους από το -9 έως το 9.

Ορισμός 1.2
(Υποσύνολα, ίσα σύνολα) *Εστω A, B δύο σύνολα. Αν κάθε στοιχείο του A είναι επίσης και στοιχείο του B, τότε το A λέγεται υποσύνολο του B και το B λέγεται υπερσύνολο του B και γράφουμε:*
$$A \subset B, \quad B \supset A.$$
Εναλλακτικά χρησιμοποιείται και ο συμβολισμός
$$A \subseteq B, \quad B \supseteq A.$$
Με άλλα λόγια, $A \subset B$, αν δεν υπάρχει στοιχείο του A που δεν ανήκει στο A.
Σε διάγραμμα Venn δυό σύνολα $B \subseteq A$ παριστάνονται όπως στο Σχήμα 1.2.



Σχήμα 1.2: Διάγραμμα Venn για $B \subseteq A$

Από αυτό προκύπτει ότι:

$$\emptyset \subset B$$

για κάθε σύνολο B. Στην περίπτωση που $A \subset B$ & $B \subset A$ τα σύνολα λέγονται *ίσα* και γράφουμε $A = B$. Με άλλα λόγια ίσα σύνολα σημαίνει ότι τα σύνολα έχουν ακριβώς τα ίδια στοιχεία.

Παράδειγμα 1.2 *1.* $\{a, b, c\} = \{c, b, a\}$.

2. Εστω ότι $A = \{x\}$. *Τότε ισχύουν τα εξής:*

(α) $x \in A$,

(β) $y \in A \Longrightarrow y = x$.

Αν $A \subset B$ & $A \neq B$ τότε το A λέγεται γνήσιο υποσύνολο του B και γράφουμε $A \subsetneqq B$. Αν το A δεν είναι υποσύνολο του B τότε γράφουμε: $A \nsubseteq B$.

✏ **1.1**
Εστω $A = \{2, \{4, 5\}, 4\}$. *Ποια από τις παρακάτω προτάσεις είναι λάθος και γιατί;*

1. $\{4, 5\} \subset A$

2. $\{4, 5\} \in A$

3. $\{\{4, 5\}\} \subset A$.

✏ **1.2**
Δίνονται τα σύνολα:

- $A = \{2, 3, 4\}$,
- $B = \{x : \ x^2 = 4 \ \& \ x > 0\}$,
- $C = \{x : \ x^2 - 6x + 8 = 0\}$,
- $D = \{x \in \mathbb{Z} : \ x \ \alpha\rho\tau\iota o\varsigma\}$.

Συμπληρώστε τα κενά με $\subset, \supset$ *ή μσ (μη συγκρίσιμα), ώστε να προκύψουν αληθείς προτάσεις.*

1. $A \ldots B$

2. $A \ldots C$

3. $B \ldots C$

4. $A \dots D$

5. $B \dots D$

6. $C \dots D$

✏ **1.3**
Βρείτε ποιά από τα παρακάτω είναι σωστά και ποιά λάθος:

1. $\{1,4,3\} \subset \{1,3,4\}$,

2. $\{4\} \subset \{\{4\}\}$,

3. $\{4\} \in \{\{4\}\}$,

4. $\emptyset \subset \{\{4\}\}$.

Ορισμός 1.3
(Δυναμοσύνολο Συνόλου) *Εστω X σύνολο. Το σύνολο που έχει σαν στοιχεία τα υποσύνολα του X λέγεται δυναμοσύνολο του X και συμβολίζεται με 2^X ή $\mathcal{P}(X)$. Δηλαδή:*

$$2^X = \mathcal{P}(X) = \{A : \ A \subset X\}.$$

Παράδειγμα 1.3
Εστω $X = \{1,2\}$. Τότε, $2^X = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

Ορισμός 1.4
(Διατεταγμένα ζεύγη) *Ένα διατεταγμένο ζεύγος είναι η τοποθέτηση δύο αντικειμένων, έστω x, y, στη σειρά. Αν πρώτο αντικείμενο ή, όπως αλλιώς το λέμε, τετμημένη, βάλουμε το x, και δεύτερο αντικείμενο ή, όπως αλλιώς το λέμε, τεταγμένη, βάλουμε το y τότε το διατεταγμένο ζεύγος συμβολίζεται με (x, y). Χαρακτηριστικό γνώρισμα των διατεταγμένων ζευγών είναι η σειρά των αντικειμένων. Έτσι ορίζουμε την ιδιότητα διατεταγμένων ζευγών να σημαίνει ισότητα και στις δύο συντεταγμένες:*

$$(x, y) = (u, v) \Longleftrightarrow x = u \ \& \ y = v.$$

Σημειώστε ότι $\{x, y\} = \{y, x\}$ ενώ $(x, y) \neq (y, x)$.

Ορισμός 1.5
(Καρτεσιανό γινόμενο συνόλων) *Εστω X, Y σύνολα. Το καρτεσιανό γινόμενο των X, Y ορίζεται να είναι το σύνολο:*

$$X \times Y = \{(x, y) : \ x \in X \ \& \ y \in Y\}.$$

Αν $X = Y$ τότε το καρτεσιανό γινόμενο γράφεται και X^2. Δηλαδή:

$$X \times X = X^2 = \{(x, y) : \ x \in X \ \& \ y \in X\}.$$

Η έννοια του διατεταγμένου ζεύγους και του καρτεσιανού γινομένου μπορεί να γενικευτεί για περισσότερα από δύο αντικείμενα και σύνολα. *Διατεταγμένη n-άδα* ονομάζεται η τοποθέτηση n αντικειμένων στη σειρά. Μία διατεταγμένη n-άδα συμβολίζεται ως εξής:

$$(x_1, x_2, ..., x_n).$$

Αν $X_1, X_2, ..., X_n$ είναι σύνολα, σαν καρτεσιανό γινόμενό τους ορίζουμε το σύνολο:

$$\Pi_{i=1}^{n} X_i = X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \dots, x_n) : \ x_1 \in X_1, x_2 \in X_2, \dots, x_n \in X_n\}.$$

Στη περίπτωση που $X_1 = X_2 = ... = X_n = X$ τότε το καρτεσιανό γινόμενο συμβολίζεται απλώς με X^n.

1.3 Σχέσεις

Ορισμός 1.6
(Προτασιακός τύπος) *Προτασιακός τύπος με πεδίο ορισμού το καρτεσιανό γινόμενο $A \times B$ δύο συνόλων A, B ονομάζεται μία έκφραση $P(x, y)$ με δύο μεταβλητές που έχει την ιδιότητα, αν αντικαταστήσουμε τις μεταβλητές x, y με ένα συγκεκριμένο ζεύγος $(a, b) \in A \times B$, η έκφραση $P(a, b)$ να γίνεται αληθής ή ψευδής πρόταση.*

Παράδειγμα 1.4
$P(x, y) =$ ο x έγραψε το μυθιστόρημα y, ορίζει ένα προτασιακό τύπο στο $A \times B$, με

$$A = \{x : \ x \ \text{συγγραφέας}\}, \quad B = \{y : \ y \ \text{μυθιστόρημα}\}.$$

Έχουμε τότε

$$P(\text{Παπαδιαμάντης, Φόνισσα}) = \text{Αληθής}$$

και

$$P(\text{Παλαμάς, Άμλετ}) = \text{Ψευδής}$$

Παράδειγμα 1.5
$P(x, y) = (x < y)$ ορίζει ένα προτασιακό τύπο πάνω στο σύνολο $\mathbb{R}^2$, αν επιτρέψουμε στα x, y να παίρνουν τιμές στο $\mathbb{R}$.

Ορισμός 1.7
(Σχέσεις) *Μια σχέση R από το A στο B είναι ένας «κανόνας» που σχετίζει ορισμένα στοιχεία του A με κάποια του B. Επειδή αυτά τα στοιχεία δημιουργούν ένα πλήθος ζευγών, πεπερασμένο ή άπειρο, μπορούμε να ορίσουμε αυστηρότερα τις σχέσεις λέγοντας ότι σχέση από το A στο B ονομάζουμε ένα οποιοδήποτε υποσύνολο R του $A \times B$.*

Παρατηρούμε ότι κάθε προτασιακός τύπος $P(x, y)$ ορίζει την εξής σχέση:

$$R = \{(a, b) \in A \times B : \ P(a, b) = \alpha\lambda\eta\theta\eta\varsigma\}.$$

Πολλές φορές αντί να γράφουμε $(a, b) \in R$, γράφουμε aRb.

Παράδειγμα 1.6
Έστω $A = \{x \in \mathbb{N} : \ x < 20\}$, $B = \{3, 6, 21\}$. Θεωρούμε τον εξής προτασιακό τύπο με πεδίο ορισμού το $A \times B$:

$$P(x, y) = \text{(ο } x \text{ είναι πολλαπλάσιο του } y\text{)}.$$

Είναι:

$$R = \{(3,3), (6,3), (9,3), (12,3), (15,3), (18,3), (6,6)(12,6), (18,6)\}.$$

Έχουμε: $12R6$, $12R3$.

Παρατηρούμε ότι τα στοιχεία του A που σχετίζονται με κάποια του B είναι τα εξής:

$$\{3, 6, 7, 9, 12, 15, 18\}.$$

Αυτά λέμε ότι αποτελούν το πεδίο ορισμού της σχέσης.

Τα στοιχεία του B που σχετίζονται με κάποια του A:

$$\{3, 6\},$$

λέμε ότι αποτελούν το σύνολο τιμών της σχέσης.

Ορισμός 1.8
(Πεδίο ορισμού, σύνολο τιμών) *Αν R είναι μια οποιαδήποτε σχέση απο ένα σύνολο A σε ένα σύνολο B το πεδίο ορισμού και το σύνολο τιμών ορίζονται ως εξής:*

$$\text{dom}\, R = \{a \in A : \exists\, b \in B\ \mu\epsilon\ (a,b) \in R\},$$

και

$$\text{range}\, R = \{b \in B : \exists a \in A \mu\epsilon\ (a,b) \in R\}.$$

Ορισμός 1.9
(Αντίστροφη σχέση) *Για κάθε σχέση R από το A στο B (δηλαδή, $R \subset A \times B$), μπορούμε να ορίσουμε την αντίστροφη σχέση R^{-1} από το B στο A ως εξής:*

$$R^{-1} = \{(y,x) : (x,y) \in R\}.$$

Από τον ορισμό R^{-1} της προκύπτει ότι: $\text{dom}\, R^{-1} = \text{range}\, R$ και $\text{range}\, R^{-1} = \text{dom}\, R$.

Ορισμός 1.10
(Σύνθεση σχέσεων) *Επίσης αν R σχέση από το A στο B και S σχέση από το B στο C τότε σύνθεση της R με την S, που την συμβολίζουμε με $S \circ R$, ορίζουμε την εξής σχέση:*

$$S \circ R = \{(x,z) : (x,y) \in R\ \&\ (y,z) \in S \gamma\iota\alpha\ \kappa\alpha\pi\omicron\iota o\ y \in B\}.$$

✏ **1.4**
Εστω $A = \{1,2,...,6\}$, $B = \{a,b,c,d\}$, $C = \{1,2,...,9\}$,

$$R = \{(1,a),(1,b),(2,c),(3,c),(5,d)\}, \quad S = \{(b,2),(d,2),(d,9)\}.$$

α) Βρείτε τα εξής:

$$S^{-1}, R^{-1}, \quad \text{dom}\, S \circ R, \quad \text{range}\, S \circ R, \quad (S \circ R)^{-1}, \quad R^{-1} \circ S^{-1}.$$

β) Παρατηρήστε ότι:

$$\text{dom}\, S \circ R \subset \text{dom}\, R, \quad \text{range}\, S \circ R \subset \text{range}\, S, \quad (S \circ R)^{-1} = R^{-1} \circ S^{-1}.$$

Δικαιολογήστε ότι τα παραπάνω ισχύουν πάντα, δηλαδή για οποιαδήποτε σύνολα A, B, C και οποιεσδήποτε σχέσεις $R \subset A \times B$, $S \subset B \times C$.
💡 $S \circ R = \{(1,2),(5,2),(5,9)\}$, $R^{-1} = \{(a,1),(b,1),(c,2),(c,3),(d,5)\}$.

1.4 Συναρτήσεις

Συνάρτηση f απο το σύνολο A στο σύνολο B ονομάζεται κάθε «κανόνας» ο οποίος σε κάποια στοιχεία του A (τα οποία, ως γνωστό, λέμε ότι αποτελούν το *πεδίο ορισμού* της f) αντιστοιχεί ένα ακριβώς στοιχείο του B. Έτσι μία συνάρτηση ορίζει ένα σύνολο από ζευγάρια αντιστοίχων τιμών (ο λεγόμενος *πίνακας τιμών* ή *γράφημα* της f). Χρησιμοποιώντας την έννοια της σχέσης,μπορούμε να ορίσουμε αυστηρότερα την έννοια της συνάρτησης.

Ορισμός 1.11
(Συνάρτηση) *Συνάρτηση f από το A στο B ονομάζουμε μία σχέση $f \subset A \times B$ με την εξής ιδιότητα:*

Για κάθε $x \in \text{dom}\, f$ το σύνολο $\{y \in B : (x,y) \in f\}$ είναι μονοσύνολο.

Ως συνήθως αντί $(x,y) \in f$ γράφουμε $y = f(x)$.

Παράδειγμα 1.7
Έστω $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4\}$ *και*

$$f = \{(a, 1), (b, 2), (c, 3), (a, 3)\}, \quad g = \{(a, 1), (b, 1), (c, 1)\}, \quad h = \{(a, 1), (b, 2), (c, 4), (d, 3)\}.$$

Από τις παραπάνω σχέσεις συνάρτηση είναι η g *και η* h *με* $\text{dom}\, g = \{a, b, c\}$, $\text{dom}\, h = A$.

Το σύμβολο $f : A \longrightarrow B$ δηλώνει μία συνάρτηση με πεδίο ορισμού το A. Στην περίπτωση αυτή για να ορίσουμε τη συνάρτηση γράφουμε με τι ισούται το $f(x)$ για οποιδήποτε $x \in A$.

Παράδειγμα 1.8
Έστω $A = \{x : x$ *κράτος* $\}$, $B = \{y : y$ *πόλη* $\}$. *Ορίζουμε* $f : A \longrightarrow B$ *με*

$$f(x) = \text{η πρωτεύουσα του } x.$$

Είναι, f*(Γαλλία)=Παρίσι.*

✏ **1.5**
Δίνονται οι παρακάτω σχέσεις από το $\mathbb{R}$ *στο* $\mathbb{R}$*:*

$$f = \{(x, y) : x + 3y = 1\}, \quad g = \{(x, y) : x^2 + y^2 = 1\}, \quad h = \{(x, y) : x^2 + y^2 = 1 \ \& \ y > 0\}.$$

Βρείτε ποιές από τις παραπάνω σχέσεις είναι συναρτήσεις. Στη συνέχεια βρείτε το πεδίο ορισμού των παραπάνω σχέσεων.

Ορισμός 1.12
Έστω $f : A \longrightarrow B$ *και* $E \subset A$. *Ονομάζουμε περιορισμό της* f *στο* E *την εξής συνάρτηση:*

$$f|_E = \{(x, y) : \ x \in E \ \& \ y = f(x)\}.$$

Με άλλα λόγια, $\text{dom}\, f = E$ και $f|_E(x) = f(x)$, αν $x \in E$.

Ορισμός 1.13
(Εικόνα, Αντίστροφη Εικόνα) *Αν* $X \subset A$ *και* $Y \subset B$ *ονομάζουμε εικόνα του* X *μέσω της* f *και αντίστροφη εικόνα του* Y *μέσω της* f*, τα παρακάτω σύνολα αντίστοιχα:*

$$f(X) = \{y \in B : \ y = f(x), \ x \in A\}, \quad f^{-1}(Y) = \{x \in A : \ f(x) \in Y\}.$$

Παράδειγμα 1.9
Έστω $f : A = \{a, b, c, d\} \longrightarrow B = \{1, 2, 3\}$ *με* $f(a) = f(b) = f(c) = 1$ $f(d) = 3$. *Ισχύουν:*

$$f(A) = f(\{a, d\}) = \{1, 3\}$$

και

$$f^{-1}(\{1, 2\}) = \{a, b, c\}, \quad f^{-1}(\{2\}) = \emptyset.$$

Ορισμός 1.14
Εστω f *συνάρτηση από το* A *στο* B. *Η* f *λέγεται 1-1 (ένα προς ένα), αν για* $x_1, x_2 \in \text{dom}\, f$ *με* $f(x_1) = f(x_2)$*, έχουμε ότι* $x_1 = x_2$. *Δηλαδή διαφορετικά στοιχεία του πεδίου ορισμού έχουν διαφορετικές εικόνες. Η* f *λέγεται επί αν* $\text{range}\, f = B$.

Παράδειγμα 1.10
Η συνάρτηση h *του Παρεδείγματος 1.7 και η συνάρτηση* f *του Παραδείγματος 1.8 είναι 1-1, ενώ η* g *του Παραδείγματος 1.7 δεν είναι 1-1. Επίσης από τις παραπάνω συναρτήσεις επί είναι μόνο η* h.

✏ **1.6**
Έστω f *συνάρτηση από το* A *στο* B. *Δείξτε ότι η αντίστροφη σχέση* f^{-1} *είναι συνάρτηση αν και μόνο αν η* f *είναι 1-1.*

✏ **1.7**
Έστω $f : \mathbb{R} \longrightarrow \mathbb{R}$ *με τύπο*

$$f(x) = \begin{cases} 2x-1 & \alpha\nu\ x < \frac{1}{2} \\ x^2 + x & \alpha\nu\ x \geq \frac{1}{2}. \end{cases}$$

α) Δείξτε ότι η f *είναι 1-1 και όχι επί.*

β) Βρείτε το σύνολο τιμών και την f^{-1}.

Λύση:
α) Έχουμε

$$x_1 < x_2 < \frac{1}{2} \Rightarrow 2x_1 < 2x_2 < 1 \Rightarrow 2x_1 - 1 < 2x_2 - 1 < 0.$$

Αρα

$$f(x_1) < f(x_2) < 0. \tag{1.1}$$

Ομοίως

$$\frac{1}{2} \leq x_1 < x_2 \Rightarrow \frac{3}{4} \leq f(x_1) < f(x_2) \quad . \tag{1.2}$$

Από τις (1.1), (1.2) έπεται ότι για $0 < y < \frac{3}{4}$ δεν υπάρχει $x \in \mathbb{R}$ με $f(x) = y$. Άρα η f δεν είναι επί. Επίσης εύκολα βλέπουμε ότι οι (1.1), (1.2) εξασφαλίζουν ότι ικανοποιείται ο ορισμός της 1-1 συνάρτησης.
β) Αν $\frac{3}{4} \leq y$ τότε

$$f(x) = y \Leftrightarrow x^2 + x - y = 0 \Leftrightarrow x = \frac{-1 + \sqrt{4+4y}}{2} \geq \frac{1}{2}. \tag{1.3}$$

Ομοίως αν $y < 0$ τότε

$$f(x) = y \Leftrightarrow x = \frac{y+1}{2} < \frac{1}{2}. \tag{1.4}$$

Από τις (1.1), (1.2), (1.3), (1.4) προκύπτουν οι

$$f(\mathbb{R}) = \{y \in \mathbb{R} : y < 0\ \eta'\ y \geq \frac{3}{4}\}$$

και

$$f^{-1}(y) = \frac{y+1}{2}\ \alpha\nu\ y < 0\ \kappa\alpha\iota\ f^{-1}(y) = \frac{-1+\sqrt{4+4y}}{2}\ \alpha\nu\ y \geq \frac{3}{4}.$$

Θυμίζουμε ότι από τον ορισμό τής f^{-1} ισχύει:$f^{-1}(y) = x \Leftrightarrow f(x) = y$. Επίσης $\mathrm{dom}\, f^{-1} = \mathrm{range}\, f$.

✏ **1.8**
Δίνονται οι συναρτήσεις $f, g, h : \mathbb{R} \longrightarrow \mathbb{R}$ *με τύπους*

$$f(x) = 3x - 4$$

$$g(x) = \begin{cases} x^2 + 3x & \alpha\nu\ x \geq 2 \\ x + 2 & \alpha\nu\ x < 2 \end{cases}.$$

$$h(x) = x^2 + |x|.$$

Εξετάστε αυτές τις συναρτήσεις ως προς το αν είναι 1-1 και επί.
Για την g *βρείτε τα* $g(A), g(B)$ *όπου* $A = [2, \infty)$, $B = (-\infty, 2)$ *και συμπεράνετε ότι δεν είναι επί.*

Ορισμός 1.15
(Σύνθεση συναρτήσεων) *Η σύνθεση συναρτήσεων ορίζεται όπως η σύνθεση των σχέσεων. Έστω* $f : A \longrightarrow B$, $g : B \longrightarrow C$. *Ορίζουμε* $g \circ f : A \longrightarrow C$ *την συνάρτηση* $g \circ f(x) = g(f(x))$.

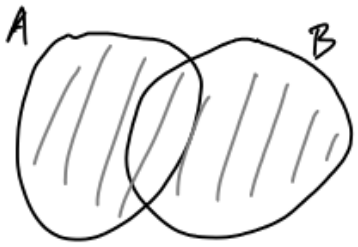
✏ **1.9**
Έστω ότι οι συναρτήσεις $f : A \longrightarrow B$, $g : B \longrightarrow C$ *είναι 1-1. Δείξτε ότι η* $g \circ f$ *είναι επίσης 1-1.*

1.5 Πράξεις σε σύνολα

Ορισμός 1.16
(Πράξεις σε σύνολα) *Αν δοθούν δύο σύνολα A, B μπορούμε να ορίσουμε τρία άλλα σύνολα ως εξής:*

1. *Την ένωση των A, B που τη συμβολίζουμε με $A \cup B$ και είναι το σύνολο που αποτελείται από τα στοιχεία του A ή του B ή και των δύο, δηλαδή:*

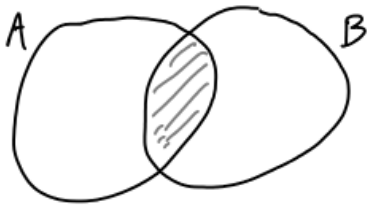
$$A \cup B = \{x : \ x \in A \, \eta' \, x \in B\}.$$



Σχήμα 1.3: Η ένωση των A, B (σκιασμένο) σε διάγραμμα Venn

2. *Την τομή των A, B που τη συμβολίζουμε με $A \cap B$ και είναι το σύνολο που αποτελείται από τα κοινά στοιχεία των A και B:*

$$A \cap B = \{x : x \in A \, \kappa\alpha\iota \, x \in B\}.$$



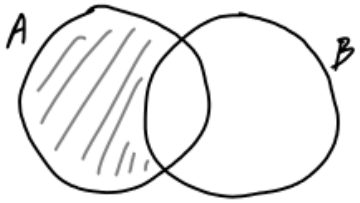
Σχήμα 1.4: Η τομή των A, B (σκιασμένο) σε διάγραμμα Venn

3. *Την διαφορά των A, B, που τη συμβολίζουμε με $A \setminus B$ και είναι το σύνολο που προκύπτει αν από τα στοιχεία του A αφαιρέσουμε εκείνα που ανήκουν στο B:*

$$A \setminus B = \{x : x \in A \, \kappa\alpha\iota \, x \notin B\}.$$

Συχνά τα σύνολα που θεωρούμε, όπως θα δούμε παρακάτω, είναι υποσύνολα ενός ευρύτερου συνόλου, έστω Ω. Στην περίπτωση αυτή ορίζουμε το συμπλήρωμα ενός $A \subset \Omega$, που το συμβολίζουμε με A^c, να είναι το σύνολο:

$$A^c = \{x \in \Omega : \ x \notin A\}.$$



Σχήμα 1.5: Η διαφορά των $A \setminus B$ (σκιασμένο) σε διάγραμμα Venn

Σχήμα 1.6: Το συμπλήρωμα του A μέσα στο Ω (σκιασμένο) σε διάγραμμα Venn

Παράδειγμα 1.11
Ρίχνουμε δύο ζάρια. Το σύνολο των δυνατών αποτελεσμάτων είναι

$$\Omega = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\} = \{(x,y) : \ x,y \in \mathbb{N} \ \& \ 1 \leq x,y \leq 6\}.$$

Το Ω αποτελείται από 36 διατεταγμένα ζεύγη. Θεωρούμε τα εξής υποσύνολα του Ω:

$$A = \{(x,y) \in \Omega : \ x+y = 7\}, \quad B = \{(x,y) \in \Omega : \ x = 6 \ \eta' \ y = 6\}.$$

Έχουμε

$$A \cap B = \{(1,6),(6,1)\},$$

$$A \cup B = \{(1,6),(2,5),(3,4),(4,3),(5,2),(6,1),(2,6),$$

$$(3,6),(4,6),(5,6),(6,6),(6,5),(6,4),(6,3),(6,2)\},$$

$$(A \cup B)^c = \{(1,1),(1,2),(1,3),(1,4),(1,5),(2,1),(2,2),(2,3),(2,4),$$

$$(3,1),(3,2),(3,3),(3,5),(4,1),(4,2),(4,4),(4,5),(5,1),(5,3),(5,4),(5,5)\}.$$

Γιά τις πράξεις μεταξύ συνόλων A, B τα οποία θεωρούμε ότι είναι υποσύνολα ενός ευρύτερου συνόλου U (το οποίο λέγεται σύνολο αναφοράς ή καθολικό σύνολο)ισχύουν οι ιδιότητες που καταγράφουμε στον παρακάτω πίνακα.

Ιδιότητες των συνολοθεωρητικών πράξεων

1. **Νόμος Ατομικότητας**:
   α) $A \cup A = A$, β) $A \cap A = A$.

2. **Προσεταιριστικός Νόμος**:
   α) $(A \cup B) \cup C = A \cup (B \cup C)$, β)$(A \cap B) \cap C = A \cap (B \cap C)$.

3. **Μεταθετικός Νόμος**:
   α) $A \cup B = B \cup A$, β) $A \cap B = B \cap A$.

4. **Επιμεριστικός Νόμος**:
   α) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, β) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

5. **Νόμοι Ταυτότητας**:
   α) $A \cup \emptyset = A$, β) $A \cap U = A$
   α') $A \cup U = U$, β') $A \cap \emptyset = \emptyset$.

6. **Νόμοι Συμπληρώματος**:
   α) $A \cup A^c = U$, β) $A \cap A^c = \emptyset$,
   α') $(A^c)^c = A$, β') $U^c = \emptyset, \emptyset^c = U$.

7. **Νόμοι De Morgan**:
   α) $(A \cup B)^c = A^c \cap B^c$, β) $(A \cap B)^c = A^c \cup B^c$.

8. **Νόμος Διάταξης**: α) $A \supset B \Leftrightarrow A \cup B = A$, β) $A \subset B \Leftrightarrow A \cap B = A$.

Παράδειγμα 1.12
Ισχύει $(A \cup B) \cap (A \cup B^c) = A$.
Έχουμε

$$(A \cup B) \cap (A \cup B^c) = A \cup (B \cap B^c) \tag{1.5}$$

και

$$B \cap B^c = \emptyset \tag{1.6}$$

(ιδιότητα 7β). Με αντικατάσταση παίρνουμε

$$(A \cup B) \cap (A \cup B^c) = A \cup \emptyset. \tag{1.7}$$

Ομως ισχύει

$$A \cup \emptyset = A \tag{1.8}$$

(ιδιότητα 5α). Οπότε, αντικαθιστώντας την (1.8) *στην* (1.7) *προκύπτει το ζητούμενο.*

Αν σε μία σχέση με σύνολα ανταλλάξουμε τα $\cap, \cup$, τα $U, \emptyset$ και τα $\subset, \supset$ προκύπτει μία νέα σχέση που λέγεται *δυϊκή* της αρχικής.

Παρατηρούμε ότι η δυϊκή κάθε ιδιότητας του παραπάνω πίνακα είναι επίσης ιδιότητα του πίνακα. Αυτό το γεγονός έχει σαν αποτέλεσμα το επόμενο πολύ σπουδαίο θεώρημα που είναι γνωστό σαν *αρχή δυϊσμού*. Η απόδειξη του θεωρήματος αυτού είναι ουσιαστικά μια επανειλημμένη χρήση των παραπάνω κανόνων και παραλείπεται. Σε κάθε συγκεκριμένη χρήση του είναι συνήθως προφανές το πώς να πάει κανείς από μια πρόταση στη δυϊκή της και το γιατί ισχύει αυτή η ισοδυναμία.

Θεώρημα 1.1
(Αρχή δυϊσμού) *Η δυϊκή σχέση κάθε σχέσης που προκύπτει απο τις ιδιότητες των πράξεων, είναι επίσης αληθής.*

Παράδειγμα 1.13
Η δυϊκή σχέση του Παραδείγματος 1.12 είναι η $(A \cap B) \cup (A \cap B^c) = A$, *η οποία είναι επίσης αληθής από την αρχή δυϊσμού. Αν θέλουμε να την αποδείξουμε απλώς θα χρησιμοποιήσουμε τις δυϊκές ιδιότητες στην απόδειξη του Παραδείγματος 1.12.*

1.6 Γενικευμένες πράξεις συνόλων

Έστω F μία οικογένεια συνόλων, δηλαδή ένα σύνολο που τα στοιχεία του είναι επίσης σύνολα. (Λέμε «οικογένεια συνόλων» αντί για «σύνολο συνόλων» απλά επειδή είναι πιο εύηχο.) Υποθέτουμε επίσης ότι έχουμε μία συνάρτηση $A : I \longrightarrow F$, η οποία είναι 1-1 και επί. Στην περίπτωση αυτή αντι $A(i)$ γράφουμε A_i οπότε η οικογένεια F γράφεται $\{A_i : i \in I\}$ ή απλούστερα $\{A_i\}_{i \in I}$.

Ορίζουμε:

$$\bigcup F = \bigcup_{A\in F} A = \bigcup_{i\in I} A_i = \{x : \exists\, i \in I \ \mu\epsilon\ x \in A_i\}$$

και

$$\bigcap F = \bigcap_{A\in F} A = \bigcap_{i\in I} A_i = \{x : \ x \in A_i \forall\, i \in I\}.$$

Δηλαδή η ένωση $\bigcup F$ περιέχει τα στοιχεία που ανήκουν σε τουλάχιστο ένα μέλος της οικογένειας και η τομή $\bigcap F$ περιέχει τα στοιχεία που ανήκουν ταυτόχρονα σε όλα τα μέλη της οικογένειας.

Παράδειγμα 1.14
Έστω $I = \mathbb{N} = \{n : n = 1, 2, 3, \ldots\}$ *και* $A_n = [0, n] = \{x \in \mathbb{R} : \ 0 \le x \le n\}$.

Έχουμε τότε

$$\bigcup_{n\in\mathbb{N}} A_n = \{x \in \mathbb{R} : \ x \ge 0\},$$

και

$$\bigcap_{n\in\mathbb{N}} A_n = [0, 1]\,.$$

Μία σημαντική ειδική περίπτωση έχουμε όταν η οικογένεια είναι πεπερασμένη, έστω $F = \{A_1, A_2, ..., A_n\}$. Τότε οι ενώσεις και τομές γράφονται επίσης ως εξής:

$$\bigcup F = \bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup ... \cup A_n,$$

$$\bigcap F = \bigcap_{i=1}^{n} A_i = A_1 \cap ... \cap A_n.$$

Εύκολα μπορεί να αποδειχθούν οι επόμενες ιδιότητες των γενικευμένων πράξεων, την απόδειξη των οποίων αφήνουμε σαν άσκηση. Έστω $\{A_i\}_{i\in I}$ οικογένεια συνόλων και B ένα σύνολο. Έστω U ένα σύνολο αναφοράς που περιέχει τα προηγούμενα σύνολα. Τότε ισχύουν:

1. **Γενικευμένος επιμεριστικός νόμος**:

$$B \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I} (B \cap A_i).$$
$$B \cup \bigcap_{i\in I} A_i = \bigcap_{i\in I} (B \cup A_i).$$

2. **Γενικευμένοι τύποι De Morgan**:

$$\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c, \quad \left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c.$$
$$B \setminus \bigcup_{i\in I} A_i = \bigcap_{i\in I} (B \setminus A_i), \quad B \setminus \bigcap_{i\in I} A_i = \bigcup_{i\in I} (B \setminus A_i).$$

✏ **1.10**
Έστω συνάρτηση $f : X \longrightarrow Y$ *με* $X_1, X_2 \subset X$ *και* $Y_1, Y_2 \subset Y$. *Δείξτε ότι*

$$f(X_1 \setminus X_2) \supset f(X_1) \setminus f(X_2), \quad f^{-1}(Y_1 \setminus Y_2) = f^{-1}(Y_1) \setminus f^{-1}(Y_2).$$

Με παράδειγμα δείξτε ότι ο εγκλεισμός στην πρώτη σχέση μπορεί να είναι γνήσιος.

Για την απόδειξη της πρώτης σχέσης, έστω $y \in f(X_1) \setminus f(X_2)$. *Αυτό σημαίνει από τον ορισμό της πράξης της διαφοράς ότι υπάρχει* $x_1 \in X_1$ *με* $f(x_1) = y$ *και για κάθε* $x \in X_2$, $f(x) \neq y$.

✏ **1.11**
Έστω $f : A \longrightarrow B$ συνάρτηση και $\{A_i\}_{i\in I}$ οικογένεια υποσυνόλων του A, και $\{B_j\}_{j\in J}$ οικογένεια υποσυνόλων του B. Δείξτε ότι:

α)

$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i), \quad f^{-1}\left(\bigcup_{j\in J} B_j\right) = \bigcup_{j\in J} f^{-1}(B_j).$$

β)

$$f\left(\bigcap_{i\in I} A_i\right) \subset \bigcap\nolimits_{i\in I} f(A_i), \quad f^{-1}\left(\bigcap_{j\in J} B_j\right) = \bigcap_{j\in J} f^{-1}(B_j).$$

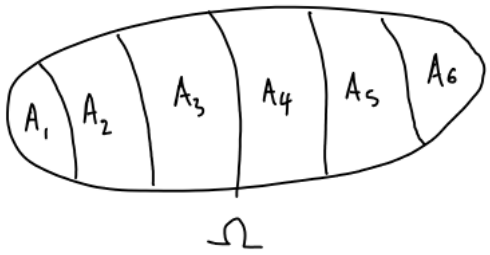
γ) Με παράδειγμα δείξτε ότι ο εγκλεισμός του ερωτήματος β) μπορεί να είναι και γνήσιος.

Γιά το ερώτημα γ) μπορείτε να θεωρήσετε ότι η οικογένεια είναι πεπερασμένη, π.χ. ότι αποτελείται από δύο σύνολα.

Κλείνουμε την παρούσα παράγραφο με την πολύ βασική ένοια της *διαμέρισης*, η οποία είναι, όπως θα δούμε στην επόμενη παράγραφο, αλληλένδετη με την ένοια της σχέσης ισοδυναμίας. Υπενθυμίζουμε πρώτα ότι δύο σύνολα λέγονται *ξένα μεταξύ τους*, αν η τομή τους ισούται με το κενό σύνολο, αν δεν έχουν δηλ. κανένα κοινό στοιχείο.

Ορισμός 1.17
(Διαμέριση) *Έστω A σύνολο και $\{A_i\}_{i\in I}$ μία οικογένεια υποσυνόλων του. Λέμε ότι η $\{A_i\}_{i\in I}$ είναι διαμέριση του A αν ισχύουν τα εξής:*

1. *$A_i \cap A_j = \emptyset$ για $i \neq j, i, j \in I$, δηλαδή τα σύνολα της οικογένειας είναι ξένα ανά δύο.*
2. *$\bigcup_{i\in I} A_i = A$.*



Σχήμα 1.7: Η διαμέριση $\Omega = \bigcup_{i=1}^{6} A_i$ σε διάγραμμα Venn

1.7 Σχέσεις ισοδυναμίας

Ορισμός 1.18
(Σχέση ισοδυναμίας) *Ας είναι X ένα σύνολο και R μια σχέση από το X στο X, δηλαδή $R \subset X \times X$. Η R λέγεται σχέση ισοδυναμίας στο X αν ισχύουν τα εξής:*

1. *$(x, x) \in R$, για κάθε $x \in X$ (Ανακλαστική ιδιότητα).*
2. *$(x, y) \in R \Rightarrow (y, x) \in R$ (Συμμετρική ιδιότητα).*
3. *$(x, y) \in R$ & $(y, z) \in R \Rightarrow (x, z) \in R$ (Μεταβατική ιδιότητα).*

Από το 1 προκύπτει ότι, αν R είναι σχέση ισοδυναμίας στο X τότε,

$$\text{dom}\, R = \text{range}\, R = X.$$

Οι περισσότερες σχέσεις ισοδυναμίας στα Μαθηματικά είναι οι λεγόμενες ισότητες. Χαρακτηριστική περίπτωση είναι η σχέση ισοδυναμίας που ορίζει την ισότητα στους ρητούς αριθμούς.

Παράδειγμα 1.15
Έστω $\mathbb{Q} = \{(a, b) : \ a \in \mathbb{Z}$ & $b \in \mathbb{N}\}$. Ως συνήθως, κάθε ρητό αντί (a, b) τον γράφουμε $\frac{a}{b}$. Ορίζουμε

$$\frac{a}{b} R \frac{c}{d} \Leftrightarrow ad = cb.$$

Εύκολα βλέπουμε ότι η ανωτέρω σχέση ικανοποιεί τον Ορισμό 1.18. Τα ισοδύναμα κλάσματα με αυτή την σχέση είναι εκείνα πού ονομάζουμε ίσα κλάσματα.

Παράδειγμα 1.16
Ας είναι $R \subset \mathbb{Z} \times \mathbb{Z}$, $R = \{(x, y) \in \mathbb{Z} : \ x - y$ διαιρείται με το 3 $\}$. Δηλαδή:

$$xRy \Leftrightarrow x - y = 3l$$

για κάποιο $l \in \mathbb{Z}$.

Εύκολα βλέπουμε ότι η σχέση αυτή είναι σχέση ισοδυναμίας (άσκηση). Λέγεται σχέση ισοδυναμίας modulo 3 στο $\mathbb{Z}$.

Ορισμός 1.19
(Κλάση ισοδυναμίας) *Έστω R σχέση ισοδυναμίας σε σύνολο X και $x \in X$. Ορίζουμε κλάση ισοδυναμίας του x, και την συμβολίζουμε με $R(x)$, το σύνολο*

$$R(x) = \{y \in X : \ xRy\}.$$

Παράδειγμα 1.17
Γιά την σχέση ισοδυναμίας του Παραδείγματος 1.15 έχουμε

$$R\left(\frac{2}{3}\right) = \left\{\frac{2}{3}, \frac{4}{6}, \frac{6}{9}, \ldots\right\}.$$

Παράδειγμα 1.18
Γιά τις κλάσεις ισοδυναμίας του Παραδείγματος 1.16 έχουμε τα παρακάτω (τις αποδείξεις τις αφήνουμε σαν άσκηση):

1. $R(1) = \{k \in \mathbb{Z} : \ k = 3l + 1 \ \gamma\iota\alpha \ \kappa\alpha\pi\omega\iota\omicron \ l \in \mathbb{Z}\}$.
2. $k \in R(1) \Rightarrow R(k) = R(1)$.
3. *Οι διαφορετικές κλάσεις ισοδυναμίας είναι οι $R(0), R(1), R(2)$ και αποτελούν διαμέριση του $\mathbb{Z}$.*

Οπως θα δούμε στο επόμενο θεώρημα οι σχέσεις ισοδυναμίας και οι διαμερίσεις είναι ταυτόσημες έννοιες: μπορεί κανείς να μιλήσει για μια διαμέριση ενός συνόλου μιλώντας για μια αντίστοιχη σχέση ισοδυναμίας που έχει τη διαμέριση αυτή ως σύνολο κλάσεων ισοδυναμίας. Ομοίως μπορεί κάποιος να μιλήσει για μια σχέση ισοδυναμίας περιγράφοντας απλά το ποια είναι η διαμέριση του συνόλου από τις κλάσεις ισοδυναμίας. Αυτό είναι το περιεχόμενο του επόμενου Θεωρήματος 1.2.

Θεώρημα 1.2
(Θεμελιώδες Θεώρημα των Σχέσεων Ισοδυναμίας) *Αν R είναι σχέση ισοδυναμίας σε ένα σύνολο X, τότε η οικογένεια των κλάσεων ισοδυναμίας $\{R(x)\}_{x \in X}$ είναι διαμέριση του X.*

Αντίστροφα, αν η οικογένεια $\{X_i\}_{i \in I}$ είναι διαμέριση του X, τότε υπάρχει σχέση ισοδυναμίας R τέτοια ώστε οι κλάσεις ισοδυναμίας της R να είναι τα σύνολα της διαμέρισης.

Αφήνουμε την απόδειξη σαν άσκηση. Γιά το αντίστροφο να πούμε ότι η σχέση ισοδυναμίας ορίζεται ως εξής:

$$xRy \Leftrightarrow x, y \in X_i \ \gamma\iota\alpha \ \kappa\alpha\pi o\iota o \ i \in I.$$

✏ **1.12**
Ας είναι $A = \{a, b, c, d\}$. Για κάθε μια από τις διαμερίσεις

$$P_1 = \{\{a\}, \{b, c, d\}\},$$

$$P_2 = \{\{a, b\}, \{c, d\}\},$$

$$P_3 = \{\{a\}, \{b\}, \{c\}, \{d\}\}$$

του A, γράψτε την αντίστοιχη σχέση ισοδυναμίας που ορίζει στο σύνολο A.

1.8 Πληθάριθμος. Αριθμήσιμα και μη άπειρα σύνολα.

Ορισμός 1.20
(Ισοδύναμα σύνολο. Πληθάριθμος.) *Δύο σύνολα A, B λέμε ότι είναι ισοδύναμα ή ότι έχουν τον ίδιο πληθάριθμο αν υπάρχει 1-1 και επί συνάρτηση $f : A \longrightarrow B$. Γράφουμε*

$$A \sim B \ \eta' \ \#A = \#B \ \eta' \ |A| = |B|.$$

Λέμε ότι το σύνολο A έχει μικρότερο πληθάριθμο από το σύνολο B αν υπάρχει συνάρτηση $f : A \longrightarrow B$ η οποία είναι 1-1 αλλά τα A και B δεν είναι ισοδύναμα. Γράφουμε

$$|A| < |B| \ \eta' \ \#A < \#B.$$

Εύκολα μπορούμε να διαπιστώσουμε ότι η σχέση μεταξύ συνόλων $\sim$, όπως την ορίσαμε παραπάνω, είναι σχέση ισοδυναμίας, δηλαδή ικανοποιεί τις τρεις ιδιότητες:

1. $A \sim A$,
2. Αν $A \sim B$ τότε $B \sim A$,
3. Αν $A \sim B$ και $B \sim C$ τότε $A \sim C$.

Παράδειγμα 1.19
Έστω $A = \{1, 2, 3\}$, $B = \{a, b, c\}, C = \{1, 2\}$. Τότε

$$\#A = \#B, \quad |C| < |B|.$$

Αν γράψουμε όλες τις συναρτήσεις απο το $C \longrightarrow B$, θα δούμε ότι καμία δέν είναι επί.

Γιά πεπερασμένα σύνολα, το αν είναι ισοδύναμα ή ίδιου πληθαρίθμου μπορούμε να το βρούμε μετρώντας τα στοιχεία τους. Τα πράγματα είναι τελείως διαφορετικά για άπειρα σύνολα, όπως θα δούμε στο επόμενο παράδειγμα και γι' αυτό τον λόγο έχουμε εισαγάγει τον προηγούμενο ορισμό για την σύγκριση των πληθαρίθμων των συνόλων και δεν είπαμε απλά ότι δύο σύνολα είναι ισοδύναμα αν έχουν τον ίδιο αριθμό στοιχείων. Αυτό το τελευταίο έχει νοήμα να το λέμε μόνο για πεπερασμένα σύνολα.

Παράδειγμα 1.20
Έστω $\mathbb{N} = \{1, 2, 3, \ldots\}$ και $A = \{2, 4, 6, \ldots\}$. Εύκολα βλέπουμε ότι η συνάρτηση $f : \mathbb{N} \longrightarrow A$, $f(x) = 2x$ είναι 1-1 και επί. Άρα

$$\mathbb{N} \sim A.$$

Στο Παράδειγμα 1.20 βλέπουμε ότι ένα άπειρο σύνολο μπορεί να είναι ισοδύναμο με ένα γνήσιο υποσυνολό του, πράγμα το οποίο δε συμβαίνει με τα πεπερασμένα σύνολα. Αυτή είναι χαρακτηριστική ιδιότητα των απείρων συνόλων, όπως θα δούμε.

Θεωρούμε τα *αρχικά τμήματα* των φυσικών αριθμών,

$$I_1 = \{1\}, I_2 = \{1, 2\}, \ldots, I_n = \{1, 2, 3, ..., n\}, \ldots .$$

Ορισμός 1.21
(Πεπερασμένο σύνολο, άπειρο σύνολο) *Ένα σύνολο A λέγεται πεπερασμένο αν είναι ισοδύναμο με κάποιο αρχικό τμήμα των φυσικών αριθμών. Αν $A \sim I_n$ τότε λέμε ότι ο πληθάριθμος ή το πλήθος στοιχείων του A ισούται με n και γράφουμε $\#A = n$ ή $\mid A \mid = n$.*

Αν ένα σύνολο δεν είναι πεπερασμένο τότε λέγεται άπειρο.

Γιά τα άπειρα σύνολα ισχύει το επόμενο θεώρημα.

Θεώρημα 1.3 *α) Ένα σύνολο είναι άπειρο αν και μόνο αν είναι ισοδύναμο με κάποιο υποσυνολό του.*

β) Αν A είναι ένα άπειρο σύνολο, τότε ισχύει

$$\mid \mathbb{N} \mid = \mid A \mid \ \eta' \ \mid \mathbb{N} \mid < \mid A \mid .$$

(Δηλαδή το μικρότερου πληθαρίθμου άπειρο σύνολο είναι το σύνολο των φυσικών αριθμών.)

γ) Αν A είναι ένα άπειρο σύνολο και $B \subset A$ με $\mid B \mid < \mid A \mid$, τότε

$$\mid A \setminus B \mid = \mid A \mid .$$

Η απόδειξη του παραπάνω θεωρήματος μπορεί να βρεθεί σε ένα οποιδήποτε βιβλίο Θεωρίας Συνόλων, π.χ. στο Halmos 1960 και δεν περιγράφεται εδώ.

Ορισμός 1.22
(Αριθμήσιμο σύνολο) *Ένα σύνολο λέγεται άπειρα αριθμήσιμο αν είναι ισοδύναμο με το σύνολο των φυσικών αριθμών $\mathbb{N}$. Ένα σύνολο λέγεται αριθμήσιμο αν είναι άπειρα αριθμήσιμο ή πεπερασμένο. Λέγεται μη αριθμήσιμο ή υπεραριθμήσιμο αν δεν είναι αριθμήσιμο.*

Παρατήρηση 1.1 *1. Αποδεικνύεται ότι*

$$|\mathbb{N}| < |\mathbb{R}| = |I|,$$

όπου I ένα οποιοδήποτε διάστημα, π.χ. $I = [0, 1]$, ή $I = (-2, 7]$ ή $I = (1, \infty)$, κ.λ.π. Με άλλα λόγια το $\mathbb{R}$ είναι άπειρο μη αριθμήσιμο ή, όπως αλλιώς το λέμε, υπεραριθμήσιμο σύνολο.

2. Τα σύνολα A που είναι ισοδύναμα με το $\mathbb{R}$, λέμε ότι έχουν την ισχύ του συνεχούς. Γράφουμε

$$|A| = c$$

σε αυτή την περίπτωση.

Επομένως όλα τα διαστήματα $I \subseteq \mathbb{R}$ έχουν την ισχύ του συνεχούς.

3. Ο Cantor, ο οποίος ήταν ένας από τους θεμελιωτές της θεωρίας συνόλων, διατύπωσε τον ισχυρισμό, ο οποίος είναι γνωστός ως υπόθεση του συνεχούς:

«Δεν υπάρχει σύνολο A ώστε να ισχύει $|\mathbb{N}| < |A| < |\mathbb{R}|$.»

Το 1963 αποδείχθηκε ότι η υπόθεση του συνεχούς είναι ανεξάρτητη από τα άλλα αξιώματα της θεωρίας συνόλων. Θυμίζουμε ότι το ίδιο συμβαίνει στην Ευκλείδια Γεωμετρία, όπου το αξίωμα της παραλληλίας είναι ανεξάρτητο από τα υπόλοιπα αξιώματα.

Για τα αριθμήσιμα σύνολα αποδεικνύεται το επόμενο θεώρημα.

Θεώρημα 1.4 *α) Όλα τα υποσύνολα ενός αριθμήσιμου συνόλου είναι αριθμήσιμα σύνολα.*

β) Ας είναι $\{X_i\}_{i\in I}$ μια οικογένεια συνόλων με σύνολο δεικτών I αριθμήσιμο και X_i αριθμήσιμα για κάθε $i \in I$. Τότε η ένωση $\bigcup_{i\in I} X_i$ είναι αριθμήσιμο σύνολο.

✏ **1.13**
Αποδείξτε το Θεώρημα 1.4.

Για να δείξουμε ότι ένα σύνολο είναι αριθμήσιμο πρέπει να περιγράψουμε τα στοιχεία του ως μια ακολουθία (όχι απαραίτητα μόνο μια φορά το καθένα). Υποθέστε λοιπόν, π.χ. για το (α) ότι ένα σύνολο E είναι αριθμήσιμο (και άρα έχετε μια ακολουθία που απαρτίζεται από τα στοιχεία του) και για ένα σύνολο $A \subseteq E$ περιγράψτε πώς από την ακολουθία των στοιχείων του E θα πάρετε μια ακολουθία που θα απαριθμεί όλα τα στοιχεία του A. Για το (β) έχετε τα στοιχεία του κάθε X_i ως μια ακολουθία $\left\{x_j^i : \ j \in \mathbb{N}\right\}$. Δείξτε πώς από αυτές τις (αριθμήσιμες σε πλήθος) ακολουθίες θα πάρετε μια ακολουθία που θα περιέχει τα στοιχεία όλων των X_i, για κάθε $i \in I$.

Παράδειγμα 1.21
Το $\mathbb{N} \times \mathbb{N}$ είναι αριθμήσιμο.

Παρατηρούμε ότι το $\mathbb{N}$ είναι η ένωση των διαδοχικών διαστημάτων (πού αποτελούν επίσης διαμέριση του $\mathbb{N}$):

$$B_1 = \{1\}, \quad B_2 = \{2,3\}, \quad B_3 = \{4,5,6\}, \quad B_4 = \{7,8,9,10\}, \ldots.$$

Επίσης το $\mathbb{N} \times \mathbb{N}$ είναι η ένωση των παρακάτω ξένων ανα δύο συνόλων (διαγώνια αρίθμηση του $\mathbb{N} \times \mathbb{N}$):

$$Z_1 = \{(1,1)\},$$

$$Z_2 = \{(2,1),(1,2)\},$$

$$Z_3 = \{(3,1),(2,2),(1,3)\},$$

$$Z_4 = \{(4,1),(3,2),(2,3),(1,4)\},$$

$$\ldots$$

Οπότε η συνάρτηση f που ορίζεται από τον παρακάτω τύπο, αφού πρώτα γράψουμε το τυχόν $k \in \mathbb{N}$ στη μορφή

$$k = \frac{n(n-1)}{2} + l,$$

με $l \in \{0,1,\ldots,n-1\}$,

$$f : k \to f(k) = (n - l + 1, l),$$

για $n = 1, 2, ...$, είναι 1-1 και επί.

Ανάλογα μπορεί να αποδειχθεί ότι το καρτεσιανό γινόμενο πεπερασμένου πλήθους παραγόντων,

$$X_1 \times X_2 \times \cdots \times X_n,$$

οποιωνδήποτε αριθμησίμων συνόλων $X_1, X_2, ..., X_n$ είναι αριθμήσιμο.

Αντίθετα, το καρτεσιανό γινόμενο απείρου πλήθους συνόλων (άπειρα από τα οποία δεν είναι μονοσύνολα) δεν είναι αριθμήσιμο Halmos 1960.

Επίσης εύκολα βλέπουμε ότι το $\mathbb{Z}$ είναι αριθμήσιμο και, αφού έχουμε δει ότι

$$\mathbb{Q} = \{(a,b) = \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\} \subset \mathbb{Z} \times \mathbb{Z},$$

έπεται από το προηγούμενο θεώρημα ότι και το $\mathbb{Q}$ είναι αριθμήσιμο.

Τελικά από το Θεώρημα 1.4 παίρνουμε ότι το σύνολο των αρρήτων $\mathbb{R} \setminus \mathbb{Q}$ είναι υπεραριθμήσιμο αφού, αν δεν ήταν, το $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$ θα ήταν κι αυτό αριθμήσιμο.

1.9 Μαθηματική Επαγωγή

1.9.1 Η μέθοδος στην απλή της μορφή

Η μέθοδος της *μαθηματικής επαγωγής* χρησιμοποιείται για να αποδείξουμε προτάσεις οι οποίες εξαρτώνται, στην απλούστερη περίπτωση, από μια ακέραια μεταβλητή, η οποία συνήθως, αλλά όχι πάντα, συμβολίζεται με το γράμμα n. Συμβολίζουμε συνήθως με $P(n)$ την πρόταση αυτή. Έτσι, $P(0)$ σημαίνει ότι η πρόταση είναι αληθής για $n = 0$, $P(1)$ ότι είναι αληθής για $n = 1$, κ.ο.κ. Σκοπός μας είναι να δείξουμε την αλήθεια της $P(n)$, για $n \geq n_0$, όπου n_0 είναι ένας ακέραιος, συνήθως μη αρνητικός, αριθμός. Θέλουμε με άλλα λόγια να δείξουμε την αλήθεια των προτάσεων

$$P(n_0), P(n_0 + 1), P(n_0 + 2), \ldots.$$

Η μέθοδος, λοιπόν, της επαγωγής για την απόδειξη της πρότασης

$$\forall n \geq n_0 : \ P(n), \tag{1.9}$$

συνίσταται στην απόδειξη των εξής δύο προτάσεων:

$$P(n_0) \tag{1.10}$$

και

$$\forall n \geq n_0 : \ P(n) \Rightarrow P(n + 1). \tag{1.11}$$

Για να δείξουμε δηλ. ότι ισχύει η πρόταση για όλες τις τιμές του n που θέλουμε, δηλ. για $n \geq n_0$, δείχνουμε πρώτα ότι ισχύει για $n = n_0$ και επίσης δείχνουμε ότι αν ισχύει για μια τιμή του n τότε ισχύει και για την επόμενη, δηλ. για το $n + 1$. Η (1.10) ονομάζεται *αρχική* ή *βασική περίπτωση* και η (1.11) ονομάζεται *επαγωγικό βήμα*. Η υπόθεση $P(n)$ στο επαγωγικό βήμα ονομάζεται *επαγωγική υπόθεση*.

Παράδειγμα 1.22
Να δειχτεί ότι, για $n \geq 1$,

$$1 + 2 + \cdots + n = \frac{1}{2}n(n + 1). \tag{1.12}$$

Εδώ η αρχική τιμή της παραμέτρου n είναι $n = 1$, οπότε ελέγχουμε πρώτα απ' όλα αν ισχύει η πρόταση για $n = 1$. Προφανώς το αριστερό μέλος ισούται με 1 ενώ, αντικαθιστώντας, βλέπουμε ότι το ίδιο ισχύει και για το δεξί. Άρα ισχύει η βασική περίπτωση και προχωρούμε να δείξουμε το επαγωγικό βήμα.

Η επαγωγική υπόθεση είναι τώρα η (1.12) (με την υπόθεση πάντα ότι $n \geq 1$) και πρέπει χρησιμοποιώντας την να δείξουμε την ίδια πρόταση όπου το n έχει αντικατασταθεί με $n + 1$, την ισότητα δηλαδή

$$1 + 2 + \cdots + n + (n + 1) = \frac{1}{2}(n + 1)(n + 2). \tag{1.13}$$

Όμως, χρησιμοποιώντας την (1.12) (αφαιρώντας την (1.12) από την (1.13) κατά μέλη) η (1.13) είναι ισοδύναμη με την ισότητα

$$n + 1 = \frac{1}{2}(n + 1)(n + 2) - \frac{1}{2}n(n + 1)$$

που εύκολα ελέγχουμε με απλές πράξεις ότι ισχύει. Δείξαμε λοιπόν και το επαγωγικό βήμα οπότε η επαγωγική απόδειξη είναι πλήρης.

Παρατήρηση 1.2
Είναι σημαντικό να τονίσουμε ότι για να μπορεί να χρησιμοποιηθεί η μέθοδος της επαγωγής πρέπει η παράμετρος της πρότασης (n στο προηγούμενο παράδειγμα) απαραίτητα να παίρνει τιμές σε ένα σύνολο (στο προηγούμενο παράδειγμα ήταν οι φυσικοί αριθμοί) που να μπορεί να εξαντληθεί αν ξεκινήσουμε από τη βασική περίπτωση και προχωράμε κάθε φορά κατά ένα.

Έτσι δε μπορεί να χρησιμοποιηθεί η μέθοδος της επαγωγής όταν π.χ. η παράμετρος μπορεί να πάρει οποιαδήποτε πραγματική τιμή.

Ας δούμε, για παράδειγμα, την πρόταση

$$P(x) : \textit{ο πραγματικός αριθμός } x \textit{ είναι ακέραιος.}$$

Το $P(0)$ προφανώς ισχύει και το ίδιο ισχύει και η συνεπαγωγή $P(x) \Rightarrow P(x+1)$, δεν ισχύει όμως η πρόταση για όλες τις (πραγματικές) τιμές της παραμέτρου x, αλλά μόνο για όσες είναι προσιτές *από το βασικό αριθμό 0 με διαδοχικές αυξήσεις κατά 1, είναι δηλ. αληθής για τους φυσικούς αριθμούς αλλά όχι για όλους τους πραγματικούς.*

✏ **1.14**
Δείξτε επαγωγικά ότι για $n \geq 1$ ισχύει

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6} n(n+1)(2n+1). \tag{1.14}$$

Παράδειγμα 1.23
Να δειχτεί ότι $2^n > n^3$ για $n \geq 10$.

Για την αρχική τιμή $n = 10$ πρέπει να δείξουμε

$$2^{10} = 1024 > 10^3 = 1000,$$

που ισχύει.

Για το επαγωγικό βήμα υποθέτουμε ότι $n \geq 10$ και ότι $2^n > n^3$ και πρέπει να δείξουμε ότι $2^{n+1} > (n+1)^3$.

Πολλαπλασιάζοντας την επαγωγική μας υπόθεση με 2 παίρνουμε $2^{n+1} > 2n^3$. Αρκεί λοιπόν να δείξουμε ότι, για $n \geq 10$, ισχύει $2n^3 \geq (n+1)^3$. Αυτή γράφεται ισοδύναμα ως

$$(2^{1/3} n)^3 \geq (n+1)^3,$$

ή

$$2^{1/3} n \geq n + 1,$$

ή

$$n \geq \frac{1}{2^{1/3} - 1},$$

που ισχύει για $n \geq 10$ αφού ισχύει για $n = 10$ (απλές πράξεις).

✏ **1.15**
Ας δείξουμε επαγωγικά την εξής πρόταση: για κάθε σύνολο από n άλογα ($n \geq 1$) όλα έχουν το ίδιο χρώμα. Για $n = 1$ άλογο η πρόταση είναι προφανώς αληθινή. Ας δείξουμε και το επαγωγικό βήμα. Υποθέτουμε ότι ισχύει η πρόταση για n άλογα και τη δείχνουμε για $n+1$. Έστω λοιπόν άλογα $a_1, a_2, \ldots, a_n, a_{n+1}$. Από την επαγωγική υπόθεση τα n άλογα $a_1, \ldots, a_n$ έχουν όλα το ίδιο χρώμα. Επίσης από την επαγωγική υπόθεση τα n άλογα $a_2, \ldots, a_{n+1}$ έχουν όλα το ίδιο χρώμα. Άρα έχουν όλα τα άλογα το ίδιο χρώμα. (Δείτε Σχήμα 1.8.)

Πού είναι το λάθος;

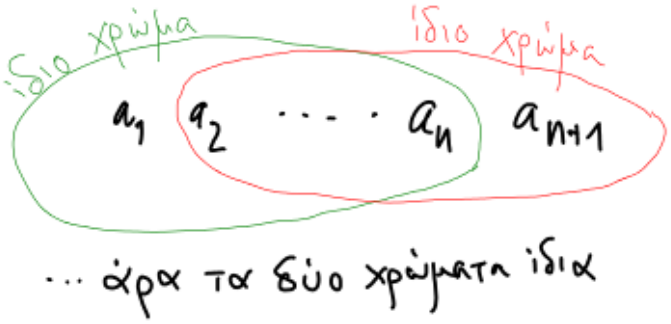
✏ **1.16**
Οι αριθμοί Fibonacci F_i, $i \geq 1$, ορίζονται αναδρομικά από

$$F_1 = F_2 = 1, \ \textit{και} \ F_n = F_{n-1} + F_{n-2} \ \textit{για} \ n > 2.$$

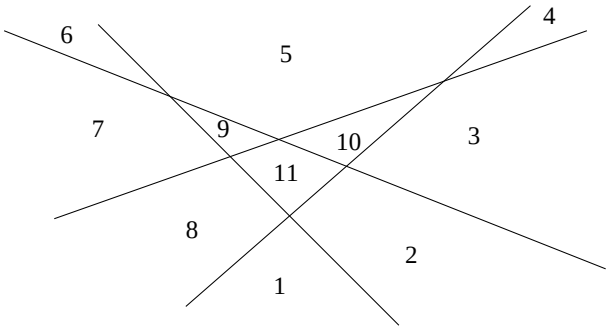
Δείξτε με επαγωγή ότι για $n \geq 1$ ο αριθμός F_{3n} είναι άρτιος.

✏ **1.17**
Για την ακολουθία Fibonacci της Άσκησης 1.16 δείξτε ότι ισχύει για $n \geq 1$

$$F_{n+2}^2 - F_{n+1}^2 = F_n F_{n+3}.$$



Σχήμα 1.8: Έχουν όλα τα άλογα το ίδιο χρώμα;



Σχήμα 1.9: Τέσσερεις ευθείες που ορίζουν 11 χωρία στο επίπεδο

✏ **1.18**
Δίνονται n ευθείες στο επίπεδο. Σε πόσα το πολύ χωρία χωρίζουν αυτές το επίπεδο; (Δείτε το Σχήμα 1.9.)

✏ **1.19**
Σε μία χώρα κάθε μια από τις $n \geq 2$ πόλεις της συνδέεται με κάθε άλλη με ένα μονόδρομο. Δηλ. αν A και B είναι δύο από τις πόλεις τότε υπάρχει είτε ο δρόμος από το A στο B είτε ο δρόμος από το B στο A, αλλά δεν ξέρουμε ποιος. Δείξτε ότι υπάρχει τρόπος να ξεκινήσει κανείς από μία πόλη της χώρας αυτής και να επισκεφτεί κάθε άλλη, ακριβώς μία φορά, κινούμενος πάνω στο υπάρχον οδικό δίκτυο (και σεβόμενος τους μονόδρομους).

✏ **1.20**
Δείξτε ότι για κάθε $x \in \mathbb{R} \setminus \{1\}$ ισχύει ο τύπος για την πεπερασμένη γεωμετρική σειρά

$$1 + x + x^2 + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x}, \quad n \geq 1. \tag{1.15}$$

Από αυτό δείξτε ότι, αν $|x| < 1$, τότε για την άπειρη γεωμετρική σειρά *ισχύει*

$$\sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots + x^n + \cdots = \frac{1}{1 - x}. \tag{1.16}$$

✏ **1.21**
Αν υποθέσαμε ότι δεν γνωρίζατε τον τύπο για την πεπερασμένη γεωμετρική σειρά της Άσκησης 1.20, πώς θα βρίσκατε ένα τύπο για το αριστερό μέλος της (1.15);
Ονομάστε A το αριστερό μέλος της (1.15) και βρείτε μια εξίσωση για το A προσθέτοντας x^{n+1} και στα δύο μέλη και εμφανίζοντας το A και στο αριστερό μέλος.

✏ **1.22**
Αποδείξτε ότι για $R > 0, n \geq 0$ ισχύει ο τύπος

$$(R(\cos x + i \sin x))^n = R^n(\cos nx + i \sin nx).$$

Εδώ i είναι ο μιγαδικός αριθμός με την ιδιότητα $i^2 = -1$. Αυτή η ιδιότητα του i αρκεί για να δείξετε το ζητούμενο (θα χρειαστείτε και τους τύπους για $\cos(a+b), \sin(a+b)$ μέσω των τριγωνομετρικών αριθμών των a, b).

✏ **1.23**
Έστω $n \geq 0$ και ότι έχουμε μια σκακιέρα με $2^n \times 2^n$ τετράγωνα από την οποία κάποιος έχει αφαιρέσει ένα τετράγωνο (την έχει τρυπήσει). Έχουμε επίσης στη διάθεσή μας απεριόριστα «τριόμινα», που είναι ξύλινα κομμάτια από 3 τετράγωνα (ίδια τετράγωνα με της σκακιέρας) σε σχήμα Γ. Αποδείξτε ότι είναι δυνατό να καλύψετε ακριβώς την τρυπημένη σκακιέρα με τριόμινα, χωρίς αυτά να αλληλοεπικαλύπτονται.

✏ **1.24**
Αποδείξτε ότι για $n \geq 1$ ο αριθμός 7 διαιρεί την ποσότητα $2^{n+2} + 3^{2n+1}$.

✏ **1.25**
Έστω ένα πολυώνυμο $f(x_1, x_2, \ldots, x_n)$ σε n πραγματικές μεταβλητές. Το πολυώνυμο γράφεται ως άθροισμα μονωνύμων με κάποιους συντελεστές και υποθέτουμε ότι δεν είναι όλοι οι συντελεστές 0. Δείξτε ότι το f δεν είναι ταυτοτικά 0, υπάρχουν δηλ. $x_1, x_2, \ldots, x_n \in \mathbb{R}^n$ τέτοια ώστε $f(x_1, x_2, \ldots, x_n) \neq 0$.

Όλες οι προηγούμενες περιπτώσεις ως επαγωγική υπόθεση

Η μέθοδος της λεγόμενης *ισχυρής μαθηματικής επαγωγής* αποδεικνύει την αλήθεια μιας πρότασης $P(n)$, για $n \geq n_0$, δείχνοντας κατ' αρχήν την αλήθεια της πρότασης $P(n_0)$ (σε αυτό ταυτίζεται με τη συνηθισμένη επαγωγή) αλλά το επαγωγικό βήμα συνίσταται στην απόδειξη της συνεπαγωγής

$$P(n_0), P(n_0+1), \ldots, P(n-1), P(n) \Rightarrow P(n+1).$$

Με άλλα λόγια, για να δείξουμε την πρόταση $P(n+1)$ μας επιτρέπεται να χρησιμοποιήσουμε την αλήθεια *όλων* των προηγουμένων περιπτώσεων, και όχι μόνο της αμέσως προηγούμενης.

Παράδειγμα 1.24
Πρώτος *λέγεται ένας φυσικός αριθμός μεγαλύτερος του 1 αν οι μόνοι διαιρέτες του είναι το 1 και ο εαυτός του. Δείχνουμε ότι κάθε φυσικός αριθμός $n \geq 2$ είναι γινόμενο πρώτων αριθμών (ισχύει και μοναδικότητα του* αναπτύγματος *αυτού αλλά δεν το αποδεικνύουμε αυτό εδώ).*

Η βασική περίπτωση είναι η $n = 2$. Αφού το 2 είναι πρώτος αριθμός η πρόταση ισχύει. Έστω τώρα $n > 2$ και ας υποθέσουμε ότι η πρόταση ισχύει για όλες τις μικρότερες τιμές. Υποθέτουμε δηλ. ότι αν $2 \leq k < n$ τότε ο φυσικός αριθμός k μπορεί να γραφεί σα γινόμενο πρώτων αριθμών. Οφείλουμε να δείξουμε, χρησιμοποιώντας αυτή την υπόθεση, οτι και ο n γράφεται σα γινόμενο πρώτων.

Αν ο n είναι πρώτος αριθμός τότε ισχύει φυσικά αυτό. Άρα μπορούμε να υποθέσουμε οτι ο n δεν είναι πρώτος. Αυτό σημαίνει ότι υπάρχει κάποιος φυσικός αριθμός k, διαφορετικός από το 1 και από το n, που διαιρεί το n. Αυτό συνεπάγεται ότι $1 < k < n$, άρα, σύμφωνα με την επαγωγική υπόθεση, οι αριθμοί k και n/k (για τον οποίο επίσης ισχύει $1 < n/k < n$) γράφονται σα γινόμενο πρώτων. Το ίδιο ισχύει συνεπώς και για τον n που ισούται με το γινόμενό τους.

✏ **1.26**
Δείξτε ότι κάθε φυσικός αριθμός $n \geq 0$ μπορεί να γραφτεί στη μορφή

$$n = n_k 2^k + n_{k-1} 2^{k-1} + \cdots + n_1 2 + n_0$$

για κάποιο φυσικό $k \geq 1$ και αριθμούς $n_0, n_1, \ldots, n_k \in \{0, 1\}$. (Αυτό ονομάζεται δυαδικό ανάπτυγμα *του n και μπορείτε εύκολα να δείξετε ότι είναι μοναδικό.)*

✏ **1.27**
Κάθε ακέραια αξία $n \geq 12$ μπορεί να φτιαχτεί με κέρματα αξίας 4 και 5.

✏ **1.28**
Η ακολουθία a_n, $n \geq 1$, ορίζεται από τους τύπους

$$a_1 = 1,\ a_2 = 3,\ a_n = a_{n-1} + a_{n-2}\ (n \geq 3).$$

Δείξτε ότι $a_n < (7/4)^n$, για $n \geq 1$.

✏ **1.29**
Η ακολουθία a_n, $n \geq 1$, ορίζεται από τους τύπους

$$a_1 = 1,\ a_2 = 1,\ a_n = a_{n-1} + a_{n-2}\ (n \geq 3).$$

Δείξτε ότι για $n \geq 1$ έχουμε $a_n = \frac{a^n - b^n}{a-b}$ όπου $a = (1+\sqrt{5})/2, b = (1-\sqrt{5})/2$

1.9.2 Προχωρημένη χρήση της επαγωγής

«Μπρος-πίσω» επαγωγή

Μερικές φορές η μέθοδος επαγωγής για την απόδειξης μιας πρότασης $P(n)$ μπορεί να τροποποιηθεί ώστε αντί για να αποδεικνύουμε το επαγωγικό βήμα $P(n) \Rightarrow P(n+1)$, πράγμα που μπορεί να είναι δύσκολο να γίνει, αποδεικνύουμε ότι η πρόταση $P(n)$ συνεπάγεται το $P(k)$ για κάποιο k πολύ μεγαλύτερο του $n+1$, αλλά ταυτόχρονα αποδεικνύουμε και ότι $P(n+1) \Rightarrow P(n)$. Μαζί αυτές οι δύο συνεπαγωγές συνεπάγονται την αλήθεια της πρότασης για όλα τα n, αφού η προς τα εμπρός συνεπαγωγή μας επιτρέπει να αποδείξουμε την ισχύ της πρότασης για μια άπειρη ακολουθία από τιμές του n ενώ με τη δεύτερη συνεπαγωγή «γυρίζουμε προς τα πίσω και γεμίζουμε τα κενά».

Παράδειγμα 1.25
Ας αποδείξουμε την ανισότητα γεωμετρικού-αριθμητικού μέσου: αν $n \geq 1$ και $a_1, a_2, \ldots, a_n \geq 0$ τότε

$$(a_1 \cdot a_2 \cdots a_n)^{1/n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n}. \tag{1.17}$$

Το αριστερό μέλος της (1.17) λέγεται γεωμετρικός μέσος *των αριθμών $a_1, a_2, \ldots, a_n$ ενώ το δεξί μέλος είναι ο* αριθμητικός τους μέσος.

Κατ' αρχήν αποδεικνύουμε την πρόταση για $n = 2$ οπότε και γίνεται

$$(a_1 a_2)^{1/2} \leq \frac{a_1 + a_2}{2},$$

η οποία, μετά από λίγες πράξεις, ανάγεται στην ανισότητα $(a_1 - a_2)^2 \geq 0$ που προφανώς ισχύει.

Δείχνουμε έπειτα ότι αν η (1.17) ισχύει για το n τότε ισχύει και για το $2n$. Πράγματι αν $a_1, a_2, \ldots, a_{2n} \geq 0$ και θέσουμε

$$A = \frac{1}{n}(a_1 + \cdots + a_n), \qquad a = (a_1 \cdot a_2 \cdots a_n)^{1/n},$$

$$B = \frac{1}{n}(a_{n+1} + \cdots + a_{2n}), \qquad b = (a_{n+1} \cdots a_{2n})^{1/n}$$

τότε από την περίπτωση 2 και την περίπτωση n έχουμε

$$\begin{aligned} \frac{a_1+\cdots+a_{2n}}{2n} &= \frac{A+B}{2} && \dagger \\ &\geq \frac{a+b}{2} && \ddagger \\ &\geq (ab)^{1/2} && * \\ &= (a_1\cdots a_{2n})^{1/(2n)} && \dagger \end{aligned}$$

(†: πράξεις, ‡: περίπτωση n, $*$: περίπτωση 2).

Μέχρι στιγμής λοιπόν έχουμε δείξει ότι η πρόταση ισχύει για όλα τα n που είναι δυνάμεις του 2. Το επόμενο βήμα είναι να αποδείξουμε ότι αν ισχύει η πρόταση για το n τότε ισχύει και για το $n-1$, και αυτό συμπληρώνει την απόδειξη για όλα τα n.

Ας υποθέσουμε λοιπόν ότι ισχύει η ανισότητα (1.17) για κάποιο n και ας είναι $a_1,\ldots,a_{n-1} \geq 0$ κάποιοι μη αρνητικοί αριθμοί. Επιλέγουμε $a_n = C := \frac{a_1+\cdots+a_{n-1}}{n-1}$, αντικαθιστούμε στην (1.17), λύνουμε ως προς C και προκύπτει το ζητούμενο (εύκολες πράξεις).

Πολλαπλή επαγωγή

Πολλές φορές η πρόταση που θέλουμε να δείξουμε εξαρτάται από περισσότερες από μία παραμέτρους. Μπορεί, για παράδειγμα, να προκειται για μια πρόταση $P(m,n)$ που εξαρτάται από δύο παραμέτρους $m,n \geq 0$. Η μέθοδος της επαγωγής μπορεί μερικές φορές να εφαρμοστεί και σε τέτοιες περιπτώσεις. Στην απλούστερη περίπτωση το πρόβλημα αντιμετωπίζεται σα μια επαλληλία μονοπαραμετρικών προβλημάτων.

Σε μια τυπική τέτοια περίπτωση αποδεικνύεται πρώτα η πρόταση $P(0,0)$, και μετά δείχνουμε τη συνεπαγωγή

$$P(m,n) \Rightarrow P(m+1,n). \tag{1.18}$$

Με μόνα αυτά τα δύο βήματα στο «οπλοστάσιό» μας δε μπορούμε ακόμη να ξεφύγουμε από τη γραμμή $n=0$. Αν όμως αποδείξουμε και τη συνεπαγωγή

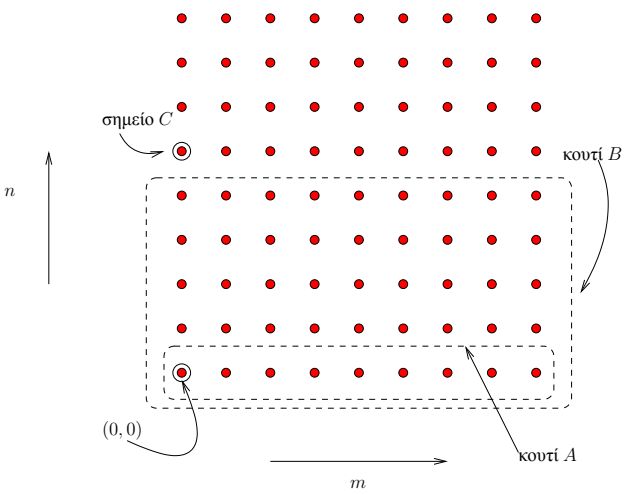
$$(\forall m \geq 0\ \forall k < n\ P(m,k)) \Rightarrow P(0,n), \tag{1.19}$$

τότε έχουμε μια πλήρη απόδειξη για όλα τα ζεύγη των τιμών (m,n).

Ας περιγράψουμε λίγο το τι σημαίνουν αυτές οι συνεπαγωγές που μοιάζουν (και είναι) αρκετά αυθαίρετες. Αυτό που θέλουμε είναι να αποδείξουμε την αλήθεια της πρότασης $P(m,n)$ σε όλα τα ακέραια σημεία του τεταρτημορίου $m,n \geq 0$ του επιπέδου. Ας αναφερθούμε στο Σχήμα 1.10 όπου παριστάνεται σχηματικά το τεταρτημόριο αυτό.

Με το βασικό βήμα της επαγωγής αποδεικνύουμε την αλήθεια της $P(\cdot,\cdot)$ στο σημείο $(0,0)$. Μετά την απόδειξη της (1.18) μπορούμε επεκτείνουμε την αλήθεια της $P(\cdot,\cdot)$ σε όλο το (ημιάπειρο) «κουτί A», που αποτελείται από όλα τα σημεία του τύπου $(\cdot,0)$. Και αυτό γιατί το νόημα της συνεπαγωγής (1.18) είναι ότι η αλήθεια της πρότασης επεκτείνεται από κάθε σημείο στο αμέσως δεξιά του.

Για να επεκτείνουμε την αλήθεια της $P(\cdot,\cdot)$ και προς τα πάνω χρειάζεται να έχουμε και ένα «κανόνα» που να συνάγει την αλήθεια της $P(\cdot,\cdot)$ σε ένα σημείο γνωρίζοντας την αλήθεια αυτής σε σημεία που είναι αυστηρά χαμηλότερα. Αυτός είναι ακριβώς ο ρόλος της συνεπαγωγής (1.19). Αν, για παράδειγμα, γνωρίζουμε ότι η P αληθεύει στο «κουτί B», δηλ. σε όλα τα σημεία του τύπου (m,k), όπου το m είναι οτιδήποτε και $k<n$, συμπεραίνουμε τότε ότι η $P(0,n)$ (στο «σημείο C») ισχύει. Με σημείο αφετηρίας τώρα το σημείο C και χρησιμοποιώντας ξανά τη συνεπαγωγή 1.18 επεκτείνουμε την αλήθεια της P στη γραμμή ακριβώς πάνω από το κουτί B. Συνεχίζοντας με αυτό τον τρόπο επ' άπειρον βλέπουμε ότι η πρόταση αληθεύει παντού στο τεταρτημόριο που μας ενδιαφέρει.



Σχήμα 1.10: Διπλή επαγωγή

Πρέπει να τονίσουμε εδώ ότι υπάρχουν πολλοί τρόποι να γίνει η επαγωγή σε παραπάνω από μία μεταβλητή, και ότι αυτός που αναφέραμε παραπάνω είναι απλά ένας από αυτούς. Αυτό που χρειάζεται σε μια εφαρμογή της επαγωγής είναι ένα επαγωγικό βήμα που να μπορεί να «καλύψει» όλο το σύνολο των τιμών που παίρνουν οι παράμετροι (m και n στον τρόπο που περιγράψαμε παραπάνω) ξεκινώντας από μερικές απλές βασικές περιπτώσεις. Ιδού ένα άλλο παράδειγμα: ας υποθέσουμε ότι οι παράμετροι m και n της πρότασής μας παίρνουν όλες τους φυσικούς αριθμούς ως τιμές και ότι μπορούμε εύκολα να αποδείξουμε την πρότασή μας αν $m = 0$ ή αν $n = 0$ (συνοριακές συνθήκες). Επίσης, για κάθε ζεύγος τιμών m και n όπου και τα δύο είναι τουλάχιστον 1, η αλήθεια της πρότασης προκύπτει από την αλήθεια της πρότασης στα σημεία $(m-1, n-1)$ και $(m-1, n)$ (τα σημεία ακριβώς αριστερά και αριστερά-κάτω από το (m, n) στο Σχήμα 1.10). Τότε η πρόταση αληθεύει για όλα τα $m, n \geq 0$ αφού για οποιοδήποτε τέτοιο ζεύγος μπορεί κανείς με διαδοχικές αναγωγές να οδηγηθεί να εξαρτάται από την αλήθεια της πρότασης στο σύνορο του τεταρτημορίου, όπου γνωρίζουμε ότι αυτή ισχύει. Δείτε και την Άσκηση 1.30.

✏ **1.30**
Η ακολουθία $a(n,k)$ ορίζεται για $n, k \geq 0$, και ικανοποιεί τα παρακάτω.

$$a(n,0) = 1, \ (n \geq 0),$$

$$a(n,k) = 0, \ (n < k),$$

και

$$a(n,k) = a(n-1,k-1) + a(n-1,k), \ (n \geq k \geq 1).$$

Δείξτε ότι για $n \geq k \geq 1$ ισχύει

$$a(n,k) = \frac{n(n-1)(n-2)\cdots(n-k+1)}{1 \cdot 2 \cdot 3 \cdots k}.$$

Ενισχύοντας την πρόταση που θέλουμε να δείξουμε

Πολλές φορές, και παρ' ότι εκ πρώτης όψεως μπορεί να φαίνεται παράδοξο, όταν πάμε να δείξουμε με επαγωγή μια πρόταση P είναι ευκολότερο να δείξουμε μια *ισχυρότερη* πρόταση Q, μια πρόταση δηλ. για την οποία να ισχύει για κάθε n η συνεπαγωγή $Q(n) \Rightarrow P(n)$.

Αυτό δεν είναι και τόσο περίεργο αν σκεφτούμε ότι στο επαγωγικό βήμα (1.11) η πρόταση P εμφανίζεται στο συμπέρασμα αλλά και στην υπόθεση. Δηλ. ναι μεν δυσκολεύουμε κάπως τη ζωή μας

(περνώντας από την P στην Q) αφού έχουμε να αποδείξουμε κάτι δυσκολότερο από πριν, ενισχύουμε όμως ταυτόχρονα και την επαγωγική μας υπόθεση οπότε δεν είναι προφανές ότι χάνουμε. Σε πολλές περιπτωσεις κερδίζουμε στην ευκολία απόδειξης.

Παράδειγμα 1.26
Να δειχτεί ότι ο αριθμός $1+3+5+\cdots+2n-1$ *(άθροισμα των πρώτων* n *περιττών φυσικών αριθμών) είναι τέλειο τετράγωνο για* $n \geq 1$.

Ας γράψουμε για απλότητα $S_n = 1+3+\cdots+2n-1$, *οπότε* $S_{n+1} = S_n + 2n + 1$. *Για* $n = 1$ *προφανώς ισχύει η πρόταση αφού* $S_1 = 1 = 1^2$.

Για το επαγωγικό βήμα υποθέτουμε ότι ισχύει $S_n = t^2$ *για κάποιο ακέραιο* t. *Έχουμε τότε*

$$S_{n+1} = S_n + 2n + 1 = t^2 + 2n + 1.$$

Δυστυχώς από δω και πέρα δεν υπάρχει τρόπος να δείξουμε ότι η ποσότητα $t^2 + 2n + 1$ *είναι τέλειο τετράγωνο.*

Αν όμως αντί να δείξουμε την πρόταση

$$P(n):\ S_n \text{ είναι τέλειο τετράγωνο,}$$

δείξουμε την ισχυρότερη πρόταση

$$Q(n):\ S_n = n^2,$$

η οποία προφανώς συνεπάγεται την $P(n)$, *τότε μας λύνονται τα χέρια, αφού παραπάνω από την επαγωγική υπόθεση* $t = n$ *και σε αυτή την περίπτωση η ποσότητα* t^2+2n+1 *είναι ίση με* $(n+1)^2$, *και έχουμε λοιπόν δείξει το επαγωγικό βήμα.*

✏ **1.31**
(Ανισότητα Bernoulli) Δείξτε με επαγωγή ως προς n *ότι για κάθε φυσικό αριθμό* $n \geq 0$ *και πραγματικό αριθμό* $x \geq -1$ *ισχύει*

$$(1+x)^n \geq 1 + nx. \tag{1.20}$$

Δοκιμάστε τώρα να δείξετε με επαγωγή την ασθενέστερη ανισότητα $(1+x)^n \geq nx$.

1.9.3 Εφαρμογή: Το θεώρημα του Γάμου (Hall)

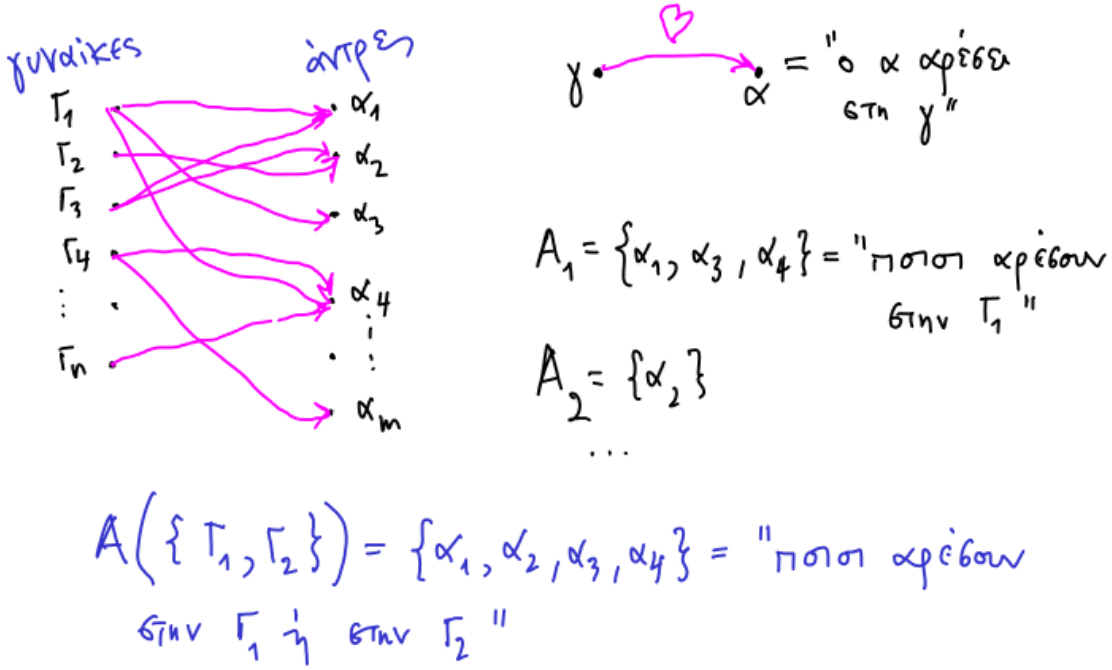
Έστω X ένα, πεπερασμένο ή άπειρο, σύνολο και $A_1, \ldots, A_n \subseteq X$ ένα *σύστημα υποσυνόλων* του X. Για απλότητα μπορούμε να θεωρήσουμε ότι το σύνολο X είναι πεπερασμένο, αν και όλες οι αποδείξεις ισχύουν και για άπειρο X (αλλά πάντα τα A_i πρέπει να είναι πεπερασμένα).

Ορισμός 1.23
(Σύστημα Ξένων Αντιπροσώπων) *Τα στοιχεία* $x_1 \in A_1, \ldots, x_n \in A_n$ *ονομάζονται ένα Σύστημα Ξένων Αντιπροσώπων (ΣΞΑ) για το σύστημα συνόλων* $A_1, \ldots, A_n$ *αν τα* $x_1, \ldots, x_n$ *είναι όλα διαφορετικά.*

Το πρόβλημα που θα μας απασχολήσει είναι να βρούμε συνθήκες για την ύπαρξη ενός ΣΞΑ για ένα σύστημα συνόλων

$$\mathcal{F} = \{A_1, \ldots, A_n\}.$$

Η ονομασία «θεώρημα του Γάμου» προέρχεται από την εξής αναλογία: υποθέτουμε ότι έχουμε n γυναίκες $\Gamma_1, \ldots, \Gamma_n$ και ότι A_i είναι το σύνολο των ανδρών που αποδέχεται η γυναίκα Γ_i ως συζύγους. (Δείτε το Σχήμα 1.11.) Το ερώτημα είναι πότε μπορούμε να διαλέξουμε από ένα σύζυγο για κάθε γυναίκα, από αυτούς που αποδέχεται, και διαφορετικό για κάθε γυναίκα. Αυτό λοιπόν γίνεται αν και μόνο αν η οικογένεια υποσυνόλων $A_1, \ldots, A_n$ (του συνόλου όλων των ανδρών) έχει κάποιο σύστημα ξένων αντιπροσώπων.



Σχήμα 1.11: Πώς ορίζονται τα σύνολα A_i και $A(J)$

Ορισμός 1.24
Για κάθε $J \subseteq [n] := \{1, 2, \ldots, n\}$ ορίζουμε

$$A(J) = A_{\mathcal{F}}(J) = \bigcup_{j \in J} A_j.$$

Ο δείκτης $\mathcal{F}$ θα παραλείπεται όταν δεν υπάρχει πρόβλημα σύγχυσης.

Είναι φανερό πως αν το σύστημα $\mathcal{F}$ έχει ένα ΣΞΑ $\{x_1, \ldots, x_n\}$ τότε έχουμε

$$\forall J \subseteq [n]: \quad |A(J)| \geq |J|. \tag{1.21}$$

Αυτό γιατί το σύνολο $A(J)$ περιέχει τουλάχιστον τα $x_j, j \in J$, τα οποία εξ ορισμού είναι όλα διαφορετικά.

Η συνθήκη (1.21) λέγεται συνθήκη του Hall και το επόμενο θεώρημα μας λέει ότι εκτός από αναγκαία είναι και ικανή για την ύπαρξη ενός ΣΞΑ για το σύστημα συνόλων $\mathcal{F}$.

Θεώρημα 1.5
(Το θεώρημα του Γάμου)
Το σύστημα συνόλων $\mathcal{F}$ έχει ΣΞΑ αν και μόνο αν ισχύει η συνθήκη του Hall (1.21).

Απόδειξη

Επαγωγή ως πρός n. Για $n = 1$ το θεώρημα είναι προφανές. Υποθέτουμε πως ισχύει μέχρι και $n - 1$. Εστω $\mathcal{F} = \{A_1, \ldots, A_n\}$ ένα σύστημα υποσυνόλων του X που ικανοποιεί την (1.21). Ενα σύνολο $J \subset [n]$, $J \neq \emptyset, [n]$, λέγεται *κρίσιμο* αν $|A(J)| = |J|$.

Περίπτωση 1η: Δεν υπάρχει κρίσιμο σύνολο J.
Από την (1.21) το A_1 έχει τουλάχιστον ένα στοιχείο, έστω x_1. Θεωρούμε τώρα το σύστημα υποσυνόλων του $X \setminus \{x_1\}$

$$\mathcal{F}' = \{A'_2, \ldots, A'_n\},$$

με $A'_j = A_j \setminus \{x_1\}$, $j = 2, \ldots, n$. Εστω $J \subseteq \{2, \ldots, n\}$. Αφού το J δεν είναι κρίσιμο για το σύστημα $\mathcal{F}$ έχουμε

$$\begin{aligned} |A_{\mathcal{F}'}(J)| &\geq |A_{\mathcal{F}}(J)| - 1 \\ &> |J| - 1 \\ &\geq |J|, \end{aligned}$$

άρα η συνθήκη του Hall (1.21) ισχύει για το σύστημα $\mathcal{F}'$. Από την επαγωγική υπόθεση υπάρχει ένα ΣΞΑ $x_2, \ldots, x_n$ για το $\mathcal{F}'$. Είναι εύκολο τότε να δεί κανείς πως τα $x_1, x_2, \ldots, x_n$ είναι ένα ΣΞΑ για το $\mathcal{F}$.

Περίπτωση 2η: Υπάρχει κάποιο κρίσιμο σύνολο.

Εστω J ένα κρίσιμο σύνολο με το ελάχιστο δυνατό μέγεθος. Για απλούστευση μπορούμε να θεωρήσουμε ότι $J = \{1, \ldots, k\}$. Εχουμε τότε $|A(J)| = |J|$. Αφού η συνθήκη του Hall ισχύει για το σύστημα $\mathcal{F}$ είναι φανερό ότι θα ισχύει και για το σύστημα $A_1, \ldots, A_k$ υποσυνόλων του $A(J)$. Αφού $k < n$ συμπεραίνουμε από την επαγωγική υπόθεση πως υπάρχει ΣΞΑ $x_1, \ldots, x_k \in A(J)$ για τα $A_1, \ldots, A_k$.

Θα δείξουμε ότι υπάρχει και ένα ΣΞΑ για τα σύνολα $A_{k+1}, \ldots, A_n$ με όλους τους αντιπροσώπους $\notin A(J)$, και έτσι θα έχει ολοκληρωθεί η απόδειξη. Γι'αυτό θα δείξουμε ότι ισχύει η συνθήκη του Hall για το σύστημα $\mathcal{F}' = \{A'_{k+1}, \ldots, A'_n\}$ υποσυνόλων του $X \setminus A(J)$, με

$$A'_j = A_j \setminus A(J), \;\; j = k+1, \ldots, n.$$

Εστω λοιπόν $I \subseteq \{k+1, \ldots, n\}$. Πρέπει να δείξουμε $|A_{\mathcal{F}'}(I)| \geq |I|$.

Από τη συνθήκη του Hall για το αρχικό σύστημα $\mathcal{F}$ έχουμε

$$|A_{\mathcal{F}}(I \cup J)| \geq |I \cup J| = |I| + |J|.$$

Αλλά είναι φανερό ότι επίσης έχουμε

$$A_{\mathcal{F}}(I \cup J) = A_{\mathcal{F}'}(I) \cup A_{\mathcal{F}}(J),$$

όπου η ένωση είναι ξένη.

Επεται ότι

$$\begin{aligned} |A_{\mathcal{F}'}(I)| &= |A_{\mathcal{F}}(I \cup J)| - |A_{\mathcal{F}}(J)| \\ &= |A_{\mathcal{F}}(I \cup J)| - |J| \\ &\geq |I \cup J| - |J| \\ &= |I| + |J| - |J| \\ &= |I|, \end{aligned}$$

που είναι αυτό που θέλαμε να δείξουμε. Αρα το σύστημα $\mathcal{F}'$ έχει ΣΞΑ του οποίου η ένωση με το ΣΞΑ $\{x_1, \ldots, x_k\}$ του συστήματος $A_1, \ldots, A_k$, μας δίνει ένα ΣΞΑ για το αρχικό σύστημα $\mathcal{F}$.

■

1.10 Προτασιακός Λογισμός

Ορισμός 1.25

(Πρόταση) *Προτάσεις ονομάζονται εκφράσεις που περιέχουν λέξεις και σύμβολα (που έχουν οριστεί και*

έχουν νόημα), οι οποίες μπορούν να χαρακτηριστούν σαν αληθείς ή ψευδείς. Τις προτάσεις θα τις συμβολίζουμε με ένα μικρό λατινικό γράμμα (με ή χωρίς δείκτες):

$$p, q, r, p_1, \ldots$$

Παράδειγμα 1.27
Οι εκφράσεις,

$$p : \textit{κάθε ακέραιος αριθμός διαιρεί τα πολλαπλασιά του,}$$
$$q : \textit{ο Ηλιος δύει στο βορρά}$$

είναι προτάσεις, γιατί η p είναι αληθής και η q είναι ψευδής.

Δεν πρέπει να μπερδεύουμε τις εκφράσεις που είναι προτάσεις στον προτασιακό λογισμό με εκείνες που είναι προτάσεις στην κοινή γλώσσα. Χαρακτηριστική ιδιότητα για να είναι μια έκφραση πρόταση είναι να επιδέχεται ένα και μόνο ένα χαρακτηρισμό:

αληθής (α) ή ψευδής (ψ).

Παράδειγμα 1.28
Η έκφραση:

Που πηγαίνεις;

δεν είναι πρόταση, αφού δε χαρακτηρίζεται ούτε αληθής ούτε ψευδής.

Τιμή μιάς πρότασης p, λέγεται η αλήθεια ή το ψεύδος της. Γράφουμε:

$$v(p) = \alpha\ \eta'\ 1\ \eta'\ T$$

αν είναι αληθής και

$$v(p) = \psi\ \eta'\ 0\ \eta'\ F$$

αν είναι ψευδής. Καταχρηστικά (για ευκολία μας) γράφουμε επίσης καμιά φορά $p = \alpha$ ή ψ αντί να γράψουμε $v(p) = \alpha$ ή ψ.

Από μία ή περισσότερες προτάσεις μπορούμε να δημιουργήσουμε μία νέα σύνθετη πρόταση. Γιά να γινούμε πιό συγκεκριμένοι, ξεκινάμε με ορισμένα παραδείγματα.

Παράδειγμα 1.29
Θεωρούμε τις προτάσεις,

$$p : \textit{κάνει κρύο,}$$
$$q : \textit{βρέχει,}$$
$$r : \textit{ο ήλιος λάμπει.}$$

1. *Αν συνδέσουμε τις p και q με την λέξη «και», δημιουργούμε την σύνθετη πρόταση*

   $$p \wedge q : \textit{κάνει κρύο και βρέχει,}$$

   η οποία λέγεται σύζευξη *των p και q, συμβολίζεται $p \wedge q$ (διαβάζεται p και q) και η οποία είναι αληθής μόνο αν και οι δύο προτάσεις είναι αληθείς.*

2. *Με την λέξη «δεν» και την πρόταση q, δημιουργούμε μιά νέα πρόταση*

   $$\sim q : \textit{δεν βρέχει,}$$

   η οποία λέγεται άρνηση *της q, συμβολίζεται $\sim q$ (διαβάζεται όχι q) και είναι αληθής μόνο αν η q είναι ψευδής.*

3. *Αν συνδέσουμε τις προτάσεις p, r με την λέξη «ή» τότε έχουμε την σύνθετη πρόταση*

$$p \vee r : \textit{κάνει κρύο ή ο ήλιος λάμπει,}$$

που λέγεται διάζευξη *των p, r, συμβολίζεται $p \vee r$ (διαβάζεται p ή r) και είναι αληθής μόνο όταν αληθεύει μία τουλάχιστον απο τις προτάσεις p και r.*

4. *Πολλές προτάσεις, ειδικά στα μαθηματικά, είναι της μορφής «αν p τότε q». Τέτοιες προτάσεις με υπόθεση (η πρόταση p) και συμπέρασμα (η πρόταση q) λέγονται* συνεπαγωγές *και συμβολίζονται με $p \Rightarrow q$.*

$$p \Rightarrow q : \textit{αν κάνει κρύο τότε βρέχει.}$$

Μία συνεπαγωγή είναι ψευδής μόνο όταν το συμπέρασμα είναι ψευδές και η υπόθεση αληθής.

Γενικά μπορούμε να δημιουργήσουμε σύνθετες προτάσεις με όποιο τρόπο θέλουμε και να τις συμβολίζουμε όπως επιθυμούμε, αρκεί να καθορίσουμε πότε είναι αληθείς ή ψευδείς. Π.χ. ορίζουμε $p \curvearrowleft q$ να είναι η σύνθετη πρόταση που αληθεύει μόνο όταν αληθεύει η p και την διαβάζουμε: p ανεξάρτητα q. Κάθε τρόπος δημιουργίας νέας πρότασης από δοθείσες άλλες προτάσεις, λέγεται *τελεστής*. Οι βασικοί τελεστές που έχουν ενδιαφέρον και βρίσκουν εφαρμογές, είναι οι τελεστές του παραδείγματος 1.29. Οι τιμές τους ορίζονται από τους παρακάτω πίνακες, που λέγονται *πίνακες αλήθειας* των αντίστοιχων τελεστών.

Σύζευξη

Δύο οποιεσδήποτε προτάσεις p, q μπορούν να συνδεθούν με το «και» δημιουργώντας μία σύνθετη πρόταση, που λέγεται *σύζευξη* των p, q και συμβολίζεται με $p \wedge q$ (διαβάζεται p και q). Η τιμή της $p \wedge q$ εξαρτάται από τις τιμές των p, q όπως δίνεται από τον παρακάτω πίνακα (πίνακας αλήθειας της σύζευξης):

p	q	$p \wedge q$
α	α	α
α	ψ	ψ
ψ	α	ψ
ψ	ψ	ψ

Διάζευξη

Γιά κάθε δύο προτάσεις p, q με το διαζευτικό «ή» ορίζουμε μια νέα πρόταση που λέγεται *διάζευξη* των p και q και συμβολίζεται με $p \vee q$ (διαβάζεται p ή q). Ο πίνακας αλήθειας της διάζευξης είναι:

p	q	$p \vee q$
α	α	α
α	ψ	α
ψ	α	α
ψ	ψ	ψ

Άρνηση

Γιά κάθε πρόταση p μπορούμε να δημιουργήσουμε την πρόταση «δεν αληθεύει η p» ή «όχι p» που λέγεται *άρνηση* της p και συμβολίζεται με $\sim p$. Ο πίνακας αλήθειας της άρνησης είναι:

p	$\sim p$
α	ψ
ψ	α

Συνεπαγωγή

Η συνθετη πρόταση της μορφής «αν p τότε q», όπου p, q οποιεσδήποτε προτάσεις, λέγεται *συνεπαγωγή* και συμβολίζεται με $p \Rightarrow q$. Η πρόταση p ονομάζεται *υπόθεση* της συνεπαγωγής και η πρόταση p ονομάζεται *συμπέρασμα*. Ο πίνακας αλήθειας της συνεπαγωγής είναι:

p	q	$p \Rightarrow q$
α	α	α
α	ψ	ψ
ψ	α	α
ψ	ψ	α

Με άλλα λόγια, για να είναι αληθής μια συνπαγωγή πρέπει όποτε ισχύει η υπόθεση αναγκαστικά να ισχύει και το συμπέρασμα. Αν σε κάποια περίπτωση η υπόθεση ισχύει αλλά όχι το συμπέρασμα τότε η συνεπαγωγή θεωρείται ψευδής πρόταση. Αυτή είναι και η μόνο περίπτωση να θεωρηθεί μια συνεπαγωγή ψευδής. Ειδικότερα, αν η υπόθεση είναι ψευδής πρόταση τότε δεν έχουμε κανένα έλεγχο να κάνουμε. Σε αυτή την περίπτωση το συμπέρασμα μπορεί να είναι αληθές ή ψευδές χωρίς αυτό να επηρεάζει την αλήθεια της συνπεγαγωγής.

Παράδειγμα 1.30
Θεωρούμε τις προτάσεις:

$$p : \textit{η Αθήνα είναι πρωτεύουσα της Γαλλίας},$$
$$q : 2 + 2 = 4.$$

Ποιες είναι οι τιμές των προτάσεων

$$p \vee q,\ (\sim p) \wedge q,\ q \Rightarrow p,\ p \Rightarrow q;$$

1. *Έχουμε* $v(p \vee q) = \alpha$ *διότι* q *είναι αληθής (τρίτη γραμμή του πίνακα αληθείας της σύζευξης.*
2. *Επίσης* $v[(\sim p) \wedge q] = \alpha$ *διότι οι προτάσεις* $\sim p, q$ *είναι αληθείς.*
3. $v(q \Rightarrow p) = \psi$ *διότι η* q *είναι αληθής και η* p *είναι ψευδής.*
4. *Τέλος* $v(p \Rightarrow q) = \alpha$ *(τρίτη γραμμή του πίνακα αληθείας της συνεπαγωγής).*

Παράδειγμα 1.31
Πολλες σύνθετες προτάσεις, ειδικά στα Μαθηματικά, είναι της μορφής «p *αν και μόνο αν* q*» και ονομάζονται ισοδυναμίες. Γράφουμε:*

$$p \Longleftrightarrow q.$$

Τη σύνθετη πρόταση της ισοδυναμίας $p \Longleftrightarrow q$*, μπορούμε να την ορίσουμε ως εξής:*

$$p \Longleftrightarrow q = (p \Rightarrow q) \wedge (q \Rightarrow p)$$

Ακολουθεί ο πίνακας αληθείας της $p \Longleftrightarrow q$*.*

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$p \Longleftrightarrow q$
α	α	α	α	α
α	ψ	ψ	α	ψ
ψ	α	α	ψ	ψ
ψ	ψ	α	α	α

Παράδειγμα 1.32
Η αποκλειστική διάζευξη δύο προτάσεων p, q *που συμβολίζεται* $p \veebar q$*, ορίζεται ως εξής:*

p	q	$p \veebar q$
α	α	ψ
α	ψ	α
ψ	α	α
ψ	ψ	ψ

Με άλλα λόγια, η αποκλειστική διάζευξη είναι αληθής όταν μία από τις προτάσεις είναι αληθής, αλλά όχι και οι δύο, όταν δηλαδή αληθεύει ακριβώς μία από τις προτάσεις.

✏ **1.32**
Έστω οι προτάσεις

$$p : \text{αγόρασα λαχείο}, \ q : \text{κέρδισα το λαχείο}.$$

Περιγράψτε στην κοινή γλώσσα κάθε μια από τις παρακάτω προτάσεις:

$$\sim p,\ p \vee q,\ p \wedge q,\ p \Rightarrow q,\ \sim p \Rightarrow \sim q,\ \sim p \vee (p \wedge q).$$

✏ **1.33**
Παρακάτω σας δίνονται κάποιες σύνθετες προτάσεις $P, Q, \ldots$, και κάποιες απλούστερες $p, q, \ldots$. Γράψτε κάθε μια από τις σύνθετες προτάσεις χρησιμοποιώντας τις απλούστερες και λογικούς τελεστές.

Σύνθετες προτάσεις

- P : *Το μάθημα είναι δύσκολο και ο καθηγητής είναι απαιτητικός*
- Q : *Για να περάσει κανείς ένα δύσκολο μάθημα πρέπει να διαβάσει*
- R : *Αν ένα μάθημα είναι εύκολο και ο καθηγητής είναι απαιτητικός τότε για να το περάσει κανείς πρέπει να διαβάσει*
- S : *Αν ένα μάθημα είναι δύσκολο και ο καθηγητής απαιτητικός τότε είναι αδύνατο να το περάσει κανείς.*

Απλούστερες προτάσεις

- p : *Το μάθημα είναι δύσκολο*
- q : *Ο καθηγητής είναι απαιτητικός*
- r : *Περνάω το μάθημα*
- s : *Διαβάζω το μάθημα*

Ταυτολογίες και αντιφάσεις

Ορισμός 1.26
(Γενικευμμένη πρόταση) *Μια γενικευμένη πρόταση είναι μια πρόταση της οποία η τιμή αληθείας εξαρτάται από άλλες προτάσεις που υπεισέρχονται στην πρώτη ως μεταβλητές.*

Παράδειγμα 1.33
Αν p, q είναι ονόματα προτάσεων (οποιωνδήποτε προτάσεων, αυτές είναι οι μεταβλητές μας) τότε η έκφραση

$$p \wedge q \tag{1.22}$$

είναι μια γενικευμένη πρόταση.

Για να αποφανθούμε αν αυτή είναι αληθής ή ψευδής θα πρέπει να γνωρίζουμε τις τιμές των p και q, αν δηλ. αυτές οι προτάσεις είναι αληθείς ή ψευδείς. Προσέξτε ότι δε μας ενδιαφέρει το ποιες είναι οι προτάσεις p, q παρά μόνο το αν αυτές είναι αληθείς ή ψευδείς, για να αποφασίσουμε την τιμή αληθείας της γενικευμένης πρότασης (1.22).

Συχνά δίνουμε ονόματα στις γενικευμένες μας προτάσεις, περίπου όπως δίνουμε ονόματα στις συναρτήσεις αριθμών. Έτσι, π.χ., θα μπορούσαμε στην πρόταση (1.22) να δώσουμε το όνομα $C(p, q)$ γράφοντας

$$C(p, q) = p \wedge q.$$

Η πρόταση $C(p, q)$ παίρνει τιμή μόλις ξέρουμε τις τιμές των παραμέτρων της p, q. Αν κάποιος π.χ. μας πει ότι

$p =$ ο ήλιος είναι πιο μεγάλος από τη γη,
$q =$ η γη είναι πιο μεγάλη από το φεγγάρι,

τότε μπορούμε να αποφανθούμε ότι $C(p, q) = \alpha$.

Παράδειγμα 1.34
Οι επόμενες παραστάσεις είναι γενικευμένες προτάσεις με δύο μεταβλητές:

$$f(p, q) =\sim p \vee (p \Rightarrow q),$$

$$g(p, q) = (p \Leftrightarrow q) \wedge q,$$

$$h(p, q) = f(p, q) \wedge g(p, q)$$

Ας υποθέσουμε ότι κάποιος μας λεει ότι $p = \alpha$ και $q = \psi$. Τότε έπεται ότι $f(p, q) = \psi$, $g(p, q) = \psi$ και $h(p, q) = \psi$ (βεβαιωθείτε ότι καταλαβαίνετε πώς προκύπτουν αυτά).

Γενικά ένας σίγουρος (αλλά συνήθως αργός και βαρετός) τρόπος για να βρίσκουμε την τιμή μιάς γενικευμένης πρότασης, είναι να κάνουμε τον πίνακα αληθείας της. Ο πίνακας αληθείας της $f(p, q)$ του παραδείγματος 1.34 είναι ο εξής:

p	q	$\sim p$	$p \Rightarrow q$	$\sim p \vee (p \Rightarrow q)$
α	α	ψ	α	α
α	ψ	ψ	ψ	ψ
ψ	α	α	α	α
ψ	ψ	α	α	α

Ορισμός 1.27
(Ταυτολογία. Αντίφαση.) *Μια γενικευμένη πρόταση $P(p, q, \ldots)$ λέγεται ταυτολογία, αν η $P(p, q, \ldots)$ είναι αληθής για κάθε τιμή των $p, q, \ldots$. Η $P(p, q, \ldots)$ λέγεται αντίφαση αν είναι ψευδής για κάθε τιμή των $p, q, \ldots$ (διαφορετικά: η $P(p, q, \ldots)$ είναι ταυτολογία αν και μόνο αν η $\sim P(p, q, \ldots)$ είναι αντίφαση).*

Ορισμός 1.28
(Ισοδύναμες προτάσεις) *Λέμε ότι δύο γενικευμένες προτάσεις $P(p, q, \ldots)$, $Q(p, q, \ldots)$ με ίδιο αριθμό μεταβλητών είναι ισοδύναμες και γράφουμε*

$$P(p, q, \ldots) \equiv Q(p, q, \ldots),$$

αν η γενικευμένη πρόταση

$$P(p, q, \ldots) \Leftrightarrow Q(p, q, \ldots)$$

είναι ταυτολογία, αν δηλαδή οι πίνακες αληθείας τους ταυτίζονται.

Παράδειγμα 1.35
(Τύποι De Morgan) Θέλουμε να δείξουμε ότι οι παρακάτω σύνθετες προτάσεις είναι ταυτολογίες.

1. $\sim (p \vee q) \equiv \sim p \wedge \sim q$.
2. $\sim (p \wedge q) \equiv \sim p \vee \sim q$.

Ελέγχουμε για την πρώτη τους πίνακες αληθείας των δύο μελών της ισοδυναμίας, των προτάσεων δηλ. $\sim (p \vee q)$ και $\sim p \wedge \sim q$:

p	q	$\sim p$	$\sim q$	$p \vee q$	$\sim (p \vee q)$	$\sim p \wedge \sim q$
α	α	ψ	ψ	α	ψ	ψ
α	ψ	ψ	α	α	ψ	ψ
ψ	α	α	ψ	α	ψ	ψ
ψ	ψ	α	α	ψ	α	α

Βλέπουμε ότι οι πίνακες αληθείας των $\sim (p \vee q)$, $\sim p \wedge \sim q$ ταυτίζονται. Συνεπώς η $\sim (p \vee q) \Longleftrightarrow (\sim p \wedge \sim q)$ είναι ταυτολογία. Παρόμοια εργαζόμαστε για τη δεύτερη ισοδυναμία.

✏ **1.34**
Ποιες από τις παρακάτω γενικευμένες προτάσεις είναι ταυτολογίες, ποιες είναι αντιφάσεις και ποιες ούτε ταυτολογίες ούτε αντιφάσεις;

1. $p \wedge \sim p$
2. $p \vee \sim p$
3. $p \wedge \sim p \Rightarrow q$
4. $p \Rightarrow q$
5. $p \Rightarrow p$
6. $(p \vee q) \Rightarrow (q \vee p)$
7. $(p \wedge (p \Rightarrow q)) \Rightarrow q$
8. $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
9. $(p \Rightarrow q) \vee (p \Rightarrow \sim q)$
10. $(p \Rightarrow q) \vee (q \Rightarrow p)$

✏ **1.35**
Στο πρόβλημα αυτό βλέπουμε πώς υλοποιούμε διάφορους λογικούς τελεστές στη γλώσσα python. Στην python υπάρχουν ήδη ορισμένοι οι λογικοί τελεστές `and, or, not` *οι οποίοι δρουν μεταξύ εκφράσεων που έχουν λογικές τιμές* `True` *ή* `False`*. Στο παρακάτω πρόγραμμα (τρέξτε το και προσπαθήσετε να καταλάβετε πώς δουλεύει) χρησιμοποιούμε τους ήδη υπάρχοντες αυτούς τελεστές για να ορίσουμε τους τελεστές* $\Rightarrow$ *(συνεπαγωγή),* $\Leftrightarrow$ *(ισοδυναμία) και* $\veebar$ *(αποκλειστική διάζευξη (xor)).*

```
def implies(p, q):
    return q or not p

def equivalent(p, q):
    return implies(p, q) and implies(q, p)

def xor(p, q):
    return (p and not q) or (q and not p)

a = True
b = False

print "a => b is", implies(a, b)
print "b => a is", implies(b, a)
print "a <=> b is", equivalent(a, b)
print "a xor b is", xor(a, b)
```

1.11 Επαναληπτικές Ασκήσεις Κεφαλαίου

✏ **1.36**
Δείξτε ότι ο αριθμός 8 διαιρεί το $9^k - 1$ *για* $k \geq 1$.

✏ **1.37**
Δείξτε ότι για $n \geq 0$ *και* $0 \leq k \leq n$ *έχουμε*

$$\frac{d^k}{dx^k} x^n = \frac{n!}{(n-k)!} x^{n-k}.$$

✏ **1.38**
Δείξτε επαγωγικά ότι για $n \geq 1$ ισχύει

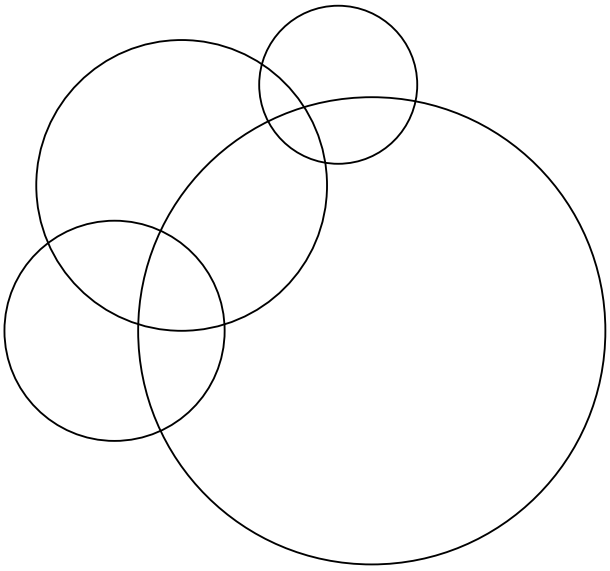
$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2. \tag{1.23}$$

✏ **1.39**
Δείξτε την ισότητα

$$\sum_{\{a_1,\ldots,a_k\}\subseteq[n]} \frac{1}{a_1 a_2 \cdots a_k} = n + 1,$$

όπου στο άθροισμα υπάρχει ακριβώς ένας προσθετέος για κάθε ένα από τα υποσύνολα $\{a_1, \ldots, a_k\}$ του $[n] = \{1, 2, \ldots, n\}$.

Σημείωση: *Ο προσθετέος στο παραπάνω άθροισμα που αντιστοιχεί στο κενό σύνολο $\{a_1, \ldots, a_k\}$ του $[n]$ είναι ο 1. Αυτό είναι φυσιολογικό γιατί το γινόμενο μηδενικού πλήθους παραγόντων είναι 1, το ουδέτερο στοιχείο του πολλαπλασιασμού, ακριβώς όπως η τιμή ενός αθροίσματος χωρίς όρους είναι 0, το ουδέτερο στοιχείο της πρόσθεσης.*



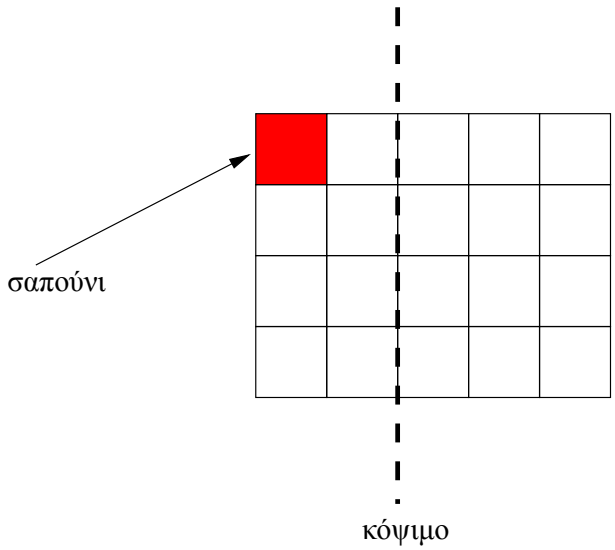
Σχήμα 1.12: Κύκλοι που ορίζουν χωρία στο επίπεδο

✏ **1.40**
Δίνονται n κύκλοι στο επίπεδο. (Δείτε το Σχήμα 1.12.) Αυτοί ορίζουν κάποια χωρία. Δείξτε ότι αυτά μπορούν να χρωματιστούν κόκκινα ή μπλέ με τέτοιο τρόπο ώστε χωρία που έχουν κοινό σύνορο (όχι απλώς κοινή γωνία αλλά ολόκληρο τόξο ως κοινό σύνορο) να έχουν διαφορετικό χρώμα.

Οι κύκλοι βρίσκονται σε γενική θέση*: κάθε δύο από αυτούς είτε τέμνονται είτε είναι ξένοι (δεν μπορούν να εφάπτονται) και δεν υπάρχουν τριπλά σημεία τομής.*

✏ **1.41**
Έχουμε μια ορθογώνια σοκολάτα που αποτελείται από τετραγωνάκια τοποθετημένα σε m γραμμές και n στήλες. Το τετραγωνάκι όμως της πάνω αριστερά γωνίας (και μόνο αυτό) είναι φτιαγμένο από σαπούνι αντί για σοκολάτα.

Δύο παίκτες παίζουν το ακόλουθο παιχνίδι. Όταν έρθει η σειρά κάποιου παίκτη αυτός κόβει ένα κομμάτι σοκολάτα και το τρώει. Η $m \times n$ σοκολάτα μπορεί να κοπεί είτε οριζόντια είτε κάθετα αλλά πλήρως, δηλ. αν η σοκολάτα κοπεί οριζόντια τότε αυτή χωρίζεται σε δύο ορθογώνιες σοκολάτες, μια $k \times n$ και



Σχήμα 1.13: Η σοκολάτα της Άσκησης 1.41 ($m = 4, n = 5$), και ένα κόψιμο από πάνω προς το κάτω.

μια $(m - k) \times n$, και ο παίκτης διαλέγει και τρώει ένα από τα δύο ορθογώνια κομμάτια. Ομοίως, αν η σοκολάτα κοπεί κάθετα τότε χωρίζεται σε δυο κομμάτια, ένα $m \times k$ και ένα $m \times (n - k)$. (Δείτε Σχήμα 1.13.)

Χάνει ο παίκτης που αναγκάζεται να φάει το τετραγωνάκι με το σαπούνι. Θα θέλατε να παίζατε πρώτος ή δεύτερος; Η απάντηση εξαρτάται από τα m και n. Βρείτε (π.χ. μαντέψτε) την απάντηση και αποδείξτε ότι έχετε δίκιο με επαγωγή ως προς το μέγεθος της σοκολάτας (mn).

✏ **1.42**

Πάνω σε έναν κυκλικό αυτοκινητόδρομο υπάρχουν n σταθμοί ανεφοδιασμού. Η συνολική ποσότητα βενζίνης που έχουν οι n σταθμοί είναι αρκετή ώστε ένα αυτοκίνητο να μπορεί να διαγράψει όλη την διαδρομή (δηλαδή έναν πλήρη κύκλο) με αυτήν. Δε κάνουμε καμία άλλη υπόθεση ούτε για το πόση βενζίνη έχει ο κάθε σταθμός ούτε και για τις μεταξύ τους αποστάσεις. Θεωρούμε οτι το αυτοκίνητο μπορεί να αποθηκεύσει απεριόριστη ποσότητα βενζίνης.

Δείξτε οτι υπάρχει κάποιος από τους n σταθμούς ανεφοδιασμού, τέτοιος ώστε αν το αυτοκίνητο ξεκινήσει από αυτόν θα μπορεί να επιστρέψει σε αυτόν (κινούμενο πάντα προς την ίδια κατεύθυνση).

✏ **1.43**

Ένας νεοεκλεγείς πρόεδρος σε μια μεγάλη χώρα με πληθυσμό από λευκούς και έγχρωμους (όλοι οι μη λευκοί) θέλει να ορίσει το υπουργικό του συμβούλιο. Θέλει να χρησιμοποιήσει αυτή του την πράξη ώστε, μεταξύ άλλων, να προωθήσει τη συνεργασία λευκών και έγχρωμων στη χώρα του. Γι' αυτό θεσπίζει τον εξής κανόνα:

> *κάθε λευκό μέλος του υπουργικού συμβουλίου θα πρέπει να έχει τουλάχιστον τόσους έγχρωμους συνεργάτες όσους και λευκούς και, ομοίως, κάθε έγχρωμο μέλος θα πρέπει να έχει τουλάχιστον τόσους λευκούς συνεργάτες όσους και έγχρωμους.*

Οι θέσεις του υπουργικού συμβουλίου είναι δεδομένες όπως και το ποιος συνεργάζεται με ποιον (π.χ. ο υπουργός Οικονομικών συνεργάζεται με όλους, ο υπουργός Άμυνας δε συνεργάζεται με τον υπουργό Γεωργίας, κλπ).

Ο ίδιος ο πρόεδρος είναι κι αυτός μέλος του υπουργικού συμβουλίου και είναι έγχρωμος.

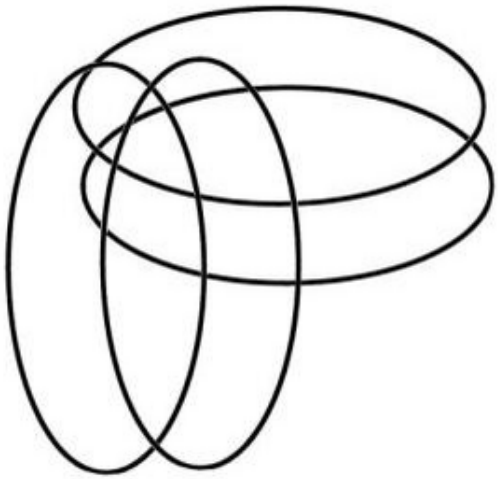
Δείξτε ότι μπορεί πάντα να επιλέξει υπουργούς του κατάλληλου χρώματος ώστε να πετύχει το σκοπό του αυτό.

Πάρτε ένα υπουργικό συμβούλιο που να μεγιστοποιεί τις συνεργασίες μεταξύ λευκών και μαύρων. Τι παρατηρείτε;

✏ **1.44**
Ας είναι $A_j \subseteq X,\ j = 1, 2, \ldots, N$, κάποια σύνολα μεγέθους k το καθένα, διαφορετικά μεταξύ τους και τέτοια ώστε η τομή οποιωνδήποτε $k+1$ από τα σύνολα A_j είναι μη κενή.

Τότε και η τομή όλων των A_j είναι μη κενή.

Υποθέστε ότι η τομή είναι κενή και καταλήξτε σε άτοπο. Αν είναι $A_1 = \{x_1, x_2, \ldots, x_k\}$ τότε θα υπάρχει κάποιο σύνολο από τα $A_2, \ldots, A_N$ που δεν περιέχει το x_1, κάποιο που δεν περιέχει το x_2, κλπ.



Σχήμα 1.14: Για την Άσκηση 1.45

✏ **1.45**
Ας είναι $\mathcal{F}$ μια πεπερασμένη οικογένεια από υποσύνολα ενός συνόλου X. Αν είναι $E \subseteq X$ ένα πεπερασμένο σύνολο μεγέθους k, λέμε ότι η οικογένεια $\mathcal{F}$ διασπά *το σύνολο E αν ο αριθμός των διαφορετικών συνόλων*

$$F \cap E$$

(όπου $F \in \mathcal{F}$), ισούται με 2^k. Όλα δηλ. τα υποσύνολα του E «φτιάχνονται» από τα σύνολα της $\mathcal{F}$ περιορισμένα στο E.

Δείξτε ότι κάθε οικογένεια $\mathcal{F}$ μεγέθους $N = |\mathcal{F}|$ διασπά τουλάχιστον N διαφορετικά υποσύνολα του X.

✏ **1.46**
Ποιες από τις παρακάτω γενικευμένες προτάσεις είναι μεταξύ τους ισοδύναμες;

1. $(p \wedge q) \vee (\sim p \wedge \sim q)$
2. $\sim p \vee q$
3. $(p \vee \sim q) \wedge (q \vee \sim p)$
4. $\sim(p \vee q)$
5. $(q \wedge p) \vee \sim p$
6. $p \Leftrightarrow q$
7. $p \Rightarrow q$
8. $q \Rightarrow p$

9. $p \vee \sim p$
10. $q \vee \sim q$

✏ **1.47**
Από μια συνηθισμένη 88 σκακιέρα έχουμε αφαιρέσει την πάνω αριστερά και την κάτω δεξιά γωνία (απομένουν δηλ. 62 τετράγωνα). Μπορείτε να καλύψετε αυτή τη σκακιέρα με ντόμινα (ζεύγη δηλ. από τετράγωνα που έχουν μια κοινή πλευρά) που όμως δεν επιτρέπεται να αλληλοεπικαλύπτονται;

1.12 Video Κεφαλαίου

1.1
Ο τύπος για το άθροισμα της γεωμετρικής σειράς. (video και συνοδευτικές ασκήσεις, 5:27 λεπτά).

Βιβλιογραφία Κεφαλαίου

[1] Paul Richard Halmos. *Naive set theory*. Springer Science & Business Media, 1960.

[2] E Kamke. *Theory of sets (translated by F. Bagemihl)*. Dover, New York, 1950.

[3] Chung Laung Liu and CL Liu. *Elements of discrete mathematics*. McGraw-Hill New York, 1985.

Κεφάλαιο 2

Θεωρία Αριθμών

Κύριες βιβλιογραφικές αναφορές για αυτό το Κεφάλαιο είναι οι Hardy and Wright 1979 και Graham, Knuth, and Patashnik 1994.

2.1 Διαιρετότητα, ισοϋπόλοιποι αριθμοί

Θεώρημα 2.1
Αν $a, b \in \mathbb{Z}$, $b > 0$, τότε υπάρχουν μοναδικοί

$$q \in \mathbb{Z},$$

(το πηλίκο), και

$$r \in \{0, 1, \ldots, b-1\},$$

(το υπόλοιπο), τέτοιοι ώστε

$$a = b \cdot q + r.$$

Ορισμός 2.1
(Διαιρετότητα, ισοϋπόλοιποι αριθμοί) *Αν το υπόλοιπο είναι 0 τότε $a = bq$ και λέμε τότε ότι ο b διαιρεί τον a. Γράφουμε $b \mid a$. Το ίδιο λέμε ακόμη και όταν ο b είναι αρνητικός (χωρίς να μιλάμε τότε για το υπόλοιπο της διαίρεσης).*

Αν δύο αριθμοί a_1, a_2 δίνουν το ίδιο υπόλοιπο r διαιρούμενοι διά b τότε λέμε ότι είναι ισοϋπόλοιποι διά b ή ισοϋπολοιποι mod$b$. *Γράφουμε επίσης σε αυτή την περίπτωση*

$$a_1 \equiv a_2 (b)$$

ή

$$a_1 = a_2 \bmod b.$$

Είναι φανερό ότι δύο ακέραιοι είναι ισοϋπόλοιποι mod$b$ *αν και μόνο αν το b διαιρεί τη διαφορά τους.*

✏ **2.1**
Υπολογίστε τα πηλίκα και υπόλοιπα των διαιρέσεων 5/3 και -5/3.

Στη γλώσσα python η πράξη / υπολογίζει το πηλίκο της διαίρεσης των δύο ακεραίων ορισμάτων της ενώ η πράξη % υπολογίζει το υπόλοιπο. Εκτελέστε και τις δύο παραπάνω διαιρέσεις στην python.

Απόδειξη

[Του Θεωρήματος 2.1:] Η ακέραια ευθεία $\mathbb{Z}$ διαμερίζεται στα σύνολα (διαστήματα) της μορφής

$$\{kb, kb+1, kb+2, \ldots, kb+(b-1)\},$$

στα διαστήματα δηλ. από το ένα πολλαπλάσιο του b στο επόμενο. Ο αριθμός a ανήκει σε ένα μοναδικό τέτοιο διάστημα, έστω στο διάστημα

$$[qb, (q+1)b) \cap \mathbb{Z}.$$

Αυτό σημαίνει ότι υπάρχει ένα $r \in \{0, 1, \ldots, b-1\}$ τέτοιο ώστε

$$a = qb + r.$$

Ας υποθέσουμε τώρα ότι το a μπορεί να γραφεί και με τη μορφή

$$a = q'b + r',$$

όπου $q' \in \mathbb{Z}$, $r \in \{0, 1, \ldots, b-1\}$. Αφαιρώντας κατά μέλη τις δύο παραπάνω σχέσεις παίρνουμε

$$r - r' = (q' - q)b,$$

δηλ. ότι ο αριθμός $r - r'$ είναι κάποιο ακέραιο πολλαπλάσιο του b. Επειδή όμως

$$0 \leq r < b, \quad 0 \leq r' < b,$$

έχουμε ότι

$$-b < r - r' < b,$$

και το μόνο πολλαπλάσιο του b σε αυτό το εύρος είναι το 0. Άρα $r = r'$ και επίσης $q = q'$, οπότε έχουμε αποδείξει και τη μοναδικότητα του ζεύγους πηλίκου, υπολοίπου πέρα από την ύπαρξη.
■

✏ **2.2**
Αποδείξτε τις παρακάτω βασικές ιδιότητες της διαιρετότητας:

1. $a \mid \pm a$
2. $a \mid b, b \mid a \Longrightarrow a = \pm b$
3. $a \mid b,\ b \mid c \Longrightarrow a \mid c$
4. $a \mid b,\ a \mid c \Longrightarrow a \mid kb + lc, \forall k, l \in \mathbb{Z}$
5. $a = b \bmod c,\ a' = b' \bmod c \Longrightarrow a \pm a' = b \pm b' \bmod c$
6. $a = b \bmod c,\ a' = b' \bmod c \Longrightarrow a \cdot a' = b \cdot b' \bmod c$

✏ **2.3**
Αν $a \mid b$ και $k \geq 1$ δείξτε $a^k \mid b^k$.

Ορισμός 2.2
(Ακέραιο μέρος, κλασματικό μέρος) *Με $\lfloor x \rfloor$ συμβολίζουμε το* ακέραιο μέρος *του πραγματικού αριθμού x, δηλ. το μεγαλύτερο ακέραιο k που ικανοποιεί $k \leq x$. Επίσης με $\{x\}$ συμβολίζουμε το* κλασματικό μέρος *του πραγματικού αριθμού x, δηλ. $\{x\} = x - \lfloor x \rfloor$.*

✏ **2.4**
Δείξτε ότι n άρτιος αν και μόνο αν $n = 2\lfloor n/2 \rfloor$.

✏ **2.5**
Πόσοι ακέραιοι ≤ 1000 δε διαιρούνται ούτε από το 3 ούτε από το 5.

✏ **2.6**
Δείξτε $3 \mid n^3 - n$.
Παραγοντοποιήστε το $n^3 - n$ πρώτα. Εναλλακτικά χρησιμοποιήστε την Άσκηση 2.2: αν r είναι το υπόλοιπο του n διά 3 τότε $n^3 - n = r^3 - r \bmod 3$ και άρα αρκεί να εξετάσετε όλα τα διαφορετικά r.

✏ **2.7**
Δείξτε ότι το τετράγωνο κάθε περιττού είναι της μορφής $8n+1$.

✏ **2.8**
Το γινόμενο δύο ακεραίων της μορφής $6n+5$ *είναι της μορφής* $6n+1$.

✏ **2.9**
Δείξτε ότι $5 \mid n^5 - n$.
Χρησιμοποιήστε την Άσκηση 2.2 και εξετάστε όλα τα δυνατά υπόλοιπα του n *διά 5.*

✏ **2.10**
Δείξτε ότι $9 \mid n^3 + (n+1)^3 + (n+2)^3$.
Μπορείτε να το λύσετε χρησιμοποιώντας και πάλι την Άσκηση 2.2. Αν βαριέστε να εξετάσετε και τις 9 περιπτώσεις τότε μπορείτε να χρησιμοποιήσετε το παρακάτω απλό πρόγραμμα σε python.

```
for r in range(9):
    k = r**3+(r+1)**3+(r+2)**3
    print k%9
```

Εναλλακτικά μπορείτε να κάνετε πράξεις στο δεξί μέλος και να χρησιμοποιήσετε την Άσκηση 2.6.

✏ **2.11**
Η ακολουθία Fibonacci ορίζεται ως εξής:

$$f_1 = f_2 = 1, \quad f_n = f_{n-1} + f_{n-2} \quad \gamma\iota\alpha\ n \geq 3.$$

Δείξτε με επαγωγή ότι:
(α) $2 \mid f_n \iff 3 \mid n$.
(β) $3 \mid f_n \iff 4 \mid n$.
(γ) $4 \mid f_n \iff 6 \mid n$.

✏ **2.12**
Δείξτε ότι $\left\lfloor (2+\sqrt{3})^n \right\rfloor$ *είναι περιττός.*
Δείξτε πρώτα χρησιμοποιώντας το διωνυμικό θεώρημα $(a+b)^N = \sum_{j=0}^{N} \binom{N}{j} a^j b^{N-j}$ *ότι*

$$(2+\sqrt{3})^n + (2-\sqrt{3})^n$$

είναι ακέραιος και μάλιστα άρτιος. Έπειτα παρατηρήστε ότι $-1 < (2-\sqrt{3})^n < 0$.

2.2 Μέγιστος κοινός διαιρέτης, ελάχιστο κοινό πολλαπλάσιο, αλγόριθμος του Ευκλείδη

Ορισμός 2.3
(Μέγιστος κοινός διαιρέτης) *Αν είναι* a, b *θετικοί ακέραιοι τότε ονομάζουμε* μέγιστο κοινό διαιρέτη *των* a, b *το μέγιστο* d *που διαιρεί και το* a *και το* b. *Το συμβολίζουμε με* (a, b).

Ορισμός 2.4
(Ελάχιστο κοινό πολλαπλάσιο) *Αν είναι* a, b *θετικοί ακέραιοι τότε ονομάζουμε* ελάχιστο κοινό πολλαπλάσιο *των* a, b *το ελάχιστο* n *τέτοιο ώστε και το* a *και το* b *διαιρούν το* n. *Το συμβολίζουμε με* $[a, b]$.

Οι παραπάνω ορισμοί γενικεύονται κατά προφανή τρόπο σε περισσότερους από δύο αριθμούς.

Παράδειγμα 2.1
Έχουμε

$$(10, 15) = 5, \ \ [10, 15] = 30.$$

Επίσης

$$(7, 11) = 1, \ \ [7, 11] = 77.$$

Για κάθε θετικό ακέραιο a έχουμε $(1, a) = 1$, $[1, a] = a$, $(a, a) = a$, $[a, a] = a$.

Θεώρημα 2.2
Αν a, b είναι δύο θετικοί ακέραιοι τότε υπάρχουν δύο ακέραιοι k, l τέτοιοι ώστε

$$(a, b) = ka + lb.$$

Απόδειξη

Έστω το σύνολο $S = \{xa + yb : \ x, y \in \mathbb{Z}\}$ όλων των ακέραιων γραμμικών συνδυασμών των a, b. Κάθε στοιχείο του S διαιρείται από το (a, b). Ας είναι d ο μικρότερος θετικός ακέραιος του S. Αν $d = ka + lb$ τότε κάθε πολλαπλάσιο του d είναι επίσης στο S. Θα δείξουμε ότι ισχύει και το αντίστροφο, ότι κάθε στοιχείο του S δηλ. είναι πολλαπλάσιο του d.

Έστω $u = xa + yb$, με $x, y \in \mathbb{Z}$ και ας γράψουμε την ακέραια διαίρεση u/d:

$$u = qd + r, \quad 0 \leq r < d.$$

Είναι φανερό ότι $r = u - qd \in S$ (αφού το S είναι κλειστό ως προς ακέραιους γραμμικούς συνδυασμούς). Αν $r > 0$ αυτό αντιφάσκει με το γεγονός ότι το d είναι το μικρότερο θετικό στοιχείο του S. Άρα $r = 0$ και $u = qd$ όπως θέλαμε να δείξουμε.

Αφού $a, b \in S$ έχουμε ότι το d διαιρεί τα a, b αλλά, από την άλλη, $(a, b) \mid d$, το οποίο σημαίνει ότι ο d είναι ένας κοινός διαιρέτης των a, b, άρα $d \leq (a, b)$. Όμως, όπως παρατηρήσαμε στην αρχή, $(a, b) \mid d$, άρα $d = (a, b)$ και άρα $(a, b) \in S$ και γράφεται ως ακέραιος γραμμικός συνδυασμός των a, b.
■

✏ **2.13**
Δείξτε ότι ο μέγιστος κοινός διαιρέτης k ακεραίων επίσης γράφεται ως ακέραιος γραμμικός συνδυασμός των ακεραίων αυτών.
Επαγωγή ως προς k και χρήση του Θεωρήματος 2.2.

Πόρισμα 2.1
Αν a, b είναι θετικοί ακέραιοι και $d \mid a, d \mid b$ τότε $d \mid (a, b)$.

Απόδειξη

Ο d διαιρεί κάθε ακέραιο γραμμικό συνδυασμό των a, b άρα και το (a, b) λόγω του Θεωρήματος 2.2.
■

Ορισμός 2.5
(Πολλαπλασιαστικό αντίστροφο mod ένα ακέραιο) *Λέμε ότι δύο ακέραιοι x, y είναι πολλαπλασιαστικά αντίστροφα* mod$b$ *αν $xy = 1 \bmod b$. Συνήθως γράφουμε $y = \overline{x}$ ή $y = x^{-1}$ αν το b υποννοείται.*

Θεώρημα 2.3
Ας είναι $a, b \geq 1$ δύο ακέραιοι. Τότε υπάρχει ακέραιος x τέτοιος ώστε $ax = 1 \bmod b$ αν και μόνο αν $(a, b) = 1$. (Υπάρχει δηλ. πολλαπλασιαστικό αντίστροφο του $a \bmod b$.)

Απόδειξη

Αν $d = (a, b) > 1$ τότε για κάθε $x \in \mathbb{Z}$ έχουμε ότι $d \nmid ax - 1$, και άρα είναι αδύνατο ο b να διαιρεί το $ax - 1$.

Αντίστροφα, αν $(a, b) = 1$ τότε από το Θεώρημα 2.2 έχουμε ότι υπάρχουν ακέραιοι x, y τέτοιοι ώστε $1 = ax + by$ απ' όπου προκύπτει ότι $ax = 1 \bmod b$.

■

✏ **2.14**

Αν x, y είναι δύο πολλαπλασιαστικά αντίστροφα mod$b$ *του a τότε $x = y \bmod b$.*

Πώς μπορείς κανείς να υπολογίσει το μέγιστο κοινό διαιρέτη δύο θετικών ακεραίων;

Λήμμα 2.1

Αν $a \geq b$ είναι δύο θετικοί ακέραιοι τότε

1. *Αν $b \mid a$ τότε $(a, b) = b$.*
2. *Αν $b \nmid a$ τότε $(a, b) = (b, r)$ όπου $r > 0$ είναι το υπόλοιπο της διαίρεσης a/b.*

Απόδειξη

Η πρώτη πρόταση είναι προφανής.

Αν $a = qb + r$ είναι η ακέραια διαίρεση a/b τότε $r = a - qb$ άρα $(a, b) \mid r$ και, αφού $(a, b) \mid b$ έπεται ότι $(a, b) \mid (b, r)$. Όμως $(b, r) \mid a$ και άρα $(b, r) \mid (a, b)$, άρα

$$(a, b) = (b, r),$$

όπως έπρεπε να δείξουμε.

■

Η προηγούμενη πρόταση είναι ουσιαστικά ο **αλγόριθμος του Ευκλείδη** για τον υπολογισμό του μέγιστου κοινού διαιρέτη δύο θετικών ακεραίων a, b. Δηλ. αντικαθιστούμε τον μεγαλύτερο από τους δύο, έστω a, από το υπόλοιπο της διαίρεσής του διά του μικροτέρου. Αν το υπόλοιπο αυτό είναι 0 (δηλ. αν $b \mid a$) τότε η απάντηση είναι b. Αλλιώς συνεχίζουμε με τον υπολογισμό του $(b, a \bmod b)$ μέχρι το $a \bmod b$ να βγει 0.

Ιδού μια υλοποίηση του αλγορίθμου αυτού στη γλώσσα python:

```
def gcd(a, b): # find the gcd of a, b, where a >= b
    print a, b
    r = a % b # if a < b then this will reverse them at the next call
    if r == 0:
        return b
    else:
        return gcd(b, r)
```

Η εντολή `print` που έχουμε βάλει ως πρώτη εντολή της συνάρτησης αυτής είναι απλά για να μας πληροφορεί ποιων αριθμών το μέγιστο κοινό διαιρέτη υπολογίζει πράγμα που μας βοηθάει να δούμε από ποιο ενδιάμεσα στάδια περνάει ο αλγόριθμος. Αν π.χ. καλέσουμε τη συνάρτηση με τους αριθμούς

$$7735, 3003$$

δίνοντας

```
print gcd(7735, 3003)
```

τότε παίρνουμε

```
7735 3003
3003 1729
1729 1274
1274 455
455 364
364 91
91
```

που είναι οι ενδιάμεσες κλήσεις στη συνάρτηση μαζί με το τελικό αποτέλεσμα (91).

2.3 Πρώτοι αριθμοί

Ορισμός 2.6
(Πρώτος αριθμός) *Ένας ακέραιος $n > 1$ λέγεται* πρώτος αριθμός *αν δεν έχει μη τετριμμένους διαιρέτες, αν δηλ.*

$$a \mid n,\ a > 1 \Longrightarrow a = n.$$

Ένας ακέραιος $n > 1$ που δεν είναι πρώτος λέγεται σύνθετος αριθμός.

Η ακολουθία των πρώτων αριθμών έχει το αρχικό κομμάτι

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, \ldots.$$

Η ακολουθία των σύνθετων αριθμών έχει το αρχικό κομμάτι

$$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34, \ldots.$$

✏ **2.15**
Ελέγξτε αν οι αριθμοί 101, 103, 107, 111, 113, 121 είναι πρώτοι.

✏ **2.16**
Αν ο $n > 1$ δεν είναι πρώτος τότε έχει κάποιο γνήσιο διαιρέτη (όχι το 1 ή το n δηλ.)

$$d <= \sqrt{n}.$$


Αφού δεν είναι πρώτος θα έχει κάποιο γνήσιο διαιρέτη k. Υποθέστε ότι $k > \sqrt{n}$ και εξετάστε το μέγεθος του n/k.

✏ **2.17**
Με βάση το αποτέλεσμα της Άσκησης 2.16 για να ελέγξουμε αν ένα θετικός ακέραιος n είναι πρώτος αρκεί να ελέγξουμε αν τον διαιρεί κάποιος από τους ακεραίους από το 2 έως τον ακέραιο $\lfloor\sqrt{n}\rfloor$. Αυτή τη μέθοδο υλοποιεί η παρακάτω συνάρτηση python.

```
def isprime(n):
    if n<=1:
        return False
    d = 2
    while d*d <= n: # Check only up to the square root of n
        if n%d == 0:
            return False
        d = d+1
    return True
```

Δοκιμάστε την παραπάνω συνάρτηση σε κάποιους αριθμούς και καταλάβετε πώς δουλεύει. Μπορείτε επίσης να υπολογίσετε όλους τους πρώτους έως το 49 με την εντολή

```
print [x for x in range(2,50) if isprime(x)]
```

οπότε παίρνετε

```
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47]
```

Την ίδια δουλειά κάνει και η παρακάτω συνάρτηση αλλά είναι κάπως πιο γρήγορη γιατί αποφεύγει να κάνει τον πολλπλασιασμό `d*d` *αντικαθιστώντας τον με μερικές προσθέσεις (που είναι συνήθως πιο γρήγορες στην υλοποίηση, ειδικά για πολύ μεγάλους αριθμούς).*

```
def isprime(n):
    if n<=1:
        return False
    d = 2
```

```
    d2 = 4
    while d2 <= n: # Check only up to the square root of n
        if n%d == 0:
            return False
        d2 = d2 + d + d +1
        d = d+1
    return True
```

Γιατί δουλεύει;

✏ **2.18**
Έστω n σύνθετος και υποθέστε ότι ο μικρότερος πρώτος παράγοντας p του n είναι $> n^{1/3}$. Δείξτε τότε ότι ο n είναι γινόμενο δύο πρώτων (όχι αναγκαστικά διαφορετικών μεταξύ τους).

Θεώρημα 2.4
Υπάρχουν άπειροι πρώτοι αριθμοί.

Απόδειξη

Ας υποθέσουμε ότι υπάρχουν πεπερασμένοι μόνο πρώτοι αριθμοί, οι $p_1, p_2, \ldots, p_n$, και έστω

$$k = p_1 p_2 \cdots p_n + 1.$$

Με βάση την υπόθεσή μας ο k δεν είναι πρώτος, άρα έχει κάποιο μη τετριμμένο διαιρέτη s, και ας υποθέσουμε ότι ο s είναι ο μικρότερος μη τετριμμένος διαιρέτης του k. Τότε ο s πρέπει να είναι πρώτος, αλλιώς θα είχε κι αυτός ένα μη τετριμμένο διαιρέτη, που θα ήταν και διαιρέτης του k και μικρότερος από τον s, πράγμα που αντιφάσκει με το ότι ο s είναι ο μικρότερος μη τετριμμένος διαιρέτης του k.

Αφού ο s είναι πρώτος τότε είναι κάποιος από τους $p_1, p_2, \ldots, p_n$, έστω $s = p_t$. Όμως $k = 1 \bmod p_t$, άτοπο.
■

✏ **2.19**
Δείξτε ότι υπάρχουν οσοδήποτε μεγάλα διαστήματα $[a, b] \subseteq \mathbb{N}$ που δεν περιέχουν πρώτους αριθμούς.
💡 *Υπάρχει πρώτος αριθμός ανάμεσα στους αριθμούς*

$$10! + 2, 10! + 3, 10! + 4, \ldots, 10! + 10;$$

✏ **2.20**
Βρείτε τους μικρότερους 5 διαδοχικούς σύνθετους ακεραίους. Βρείτε 10^6 διαδοχικούς ακεραίους που να είναι σύνθετοι.
💡 *Ο αριθμός $2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 + 2$ και οι επόμενοι 8 αριθμοί είναι όλοι σύνθετοι.*

✏ **2.21**
Ας είναι $p_1 = 2, p_2 = 3, p_3 = 5, p_4, \ldots$ οι πρώτοι αριθμοί σε αύξουσα σειρά. Χρησιμοποιώντας τη μέθοδο του Ευκλείδη (για το το ότι υπάρχουν άπειροι πρώτοι, Θεώρημα 2.4) δείξτε ότι

$$p_n \leq 2^{2^{n-1}},$$

χρησιμοποιώντας επαγωγή.

Θεώρημα 2.5
Αν p πρώτος αριθμός και $p \mid ab$ τότε $p \mid a$ ή $p \mid b$.

Απόδειξη

Έστω $ab = kp, k \in \mathbb{Z}$, και $p \nmid a$. Αφού p πρώτος αυτό σημαίνει ότι $(p, a) = 1$, και άρα, από το Θεώρημα 2.2, $1 = xa + yp$ για κάποιους $x, y \in \mathbb{Z}$. Πολλαπλασιάζοντας επί b παίρνουμε

$$b = xab + ypb = xkp + ybp = p(ak + yb)$$

άρα $p \mid b$ όπως έπρεπε να δείξουμε.
■

Παρατήρηση 2.1
Ομοίως αν $p \mid a_1 a_2 \cdots a_k$ τότε το p διαιρεί κάποιο από τα a_j (επαγωγή ως προς k).

Θεώρημα 2.6
(Θεμελιώδες Θεώρημα της Αριθμητικής) *Κάθε ακέραιος $n > 1$ μπορεί να γραφεί με μοναδικό τρόπο ως γινόμενο πρώτων αριθμών στη μορφή*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

όπου $p_1 < p_2 < \cdots < p_r$ είναι διαφορετικοί πρώτοι αριθμοί και $r, e_1, e_2, \ldots, e_r$ είναι θετικοί ακέραιοι.

Παρατήρηση 2.2
Ένας άλλος τρόπος να εκφράσει κανείς αυτό το αποτέλεσμα είναι να πει ότι για κάθε ακέραιο είναι μοναδικά καθορισμένο το ποιοι πρώτοι αριθμοί (και πόσες φορές ο καθένας) εμφανίζονται αν τον διασπάσουμε πολλαπλασιαστικά όσο περισσότερο μπορούμε. Όποτε δηλ. υπάρχει κάποιος μη τετριμμένος διαιρέτης a του αριθμού n τότε γράφουμε $n = a \cdot \frac{n}{a}$ και συνεχίζουμε διασπώντας τους δύο ακεραίους a και $\frac{n}{a}$ όσο αυτό είναι δυνατό (μέχρι αυτοί να γίνουν πρώτοι δηλαδή).

Απόδειξη

[Απόδειξη του Θεωρήματος 2.6] Είναι φανερό (ακολουθώντας την προηγούμενη παρατήρηση) ότι κάθε ακέραιος $n > 1$ μπορεί να γραφεί ως γινόμενο πρώτων. Απλά διασπάμε συνεχώς σε γινόμενο μικρότερων αριθμών, όσο μπορούμε να το κάνουμε αυτό. Όταν δε μπορούμε πλέον έχουμε φτάσει σε γινόμενο πρώτων. Αν θέλουμε μπορούμε να δώσουμε και μια πιο τυπική (αλλά όχι περισσότερο διαφωτιστική) απόδειξη με επαγωγή ως προς n.

Συνεχίζουμε με επαγωγή για τη μοναδικότητα του αναπτύγματος σε γινόμενο πρώτων.

Για $n = 2$ προφανώς ισχύει (η μικρότερη περίπτωση του n). Ας υποθέσουμε τώρα ότι ισχύει το θεώρημα για όλους τους ακεραίους μικροτερους από n και πάμε να το αποδείξουμε για το n.

Ας υποθέσουμε ότι

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

όπου $p_1, p_2, \ldots, q_1, q_2, \ldots$ πρώτοι αριθμοί, όχι κατ' ανάγκη πρώτοι μεταξύ τους. Τότε, με βάση το Θεώρημα 2.5 και την παρατήρηση που το ακολουθεί, έπεται ότι το q_1 είναι ένα από τα $q_1, q_2, \ldots$. Διαγράφοντας το p_1 και από τις δύο μεριές προκύπτει ένας μικρότερος ακέραιος $n' = n/p_1$ που γράφεται με δύο τρόπους ως γινόμενο πρώτων. Από επαγωγή αυτοί οι τρόποι πρέπει να είναι οι ίδιοι.
■

Λήμμα 2.2
Αν $a, b \geq 1$ τότε $a \mid b$ αν και μόνο αν όλοι οι πρώτοι αριθμοί που εμφανίζονται στην ανάλυση του a εμφανίζονται και στην ανάλυση του b και μάλιστα σε εκθέτη μεγαλύτερο ή ίσο από τον εκθέτη τους στον a.

Απόδειξη

Ας υποθέσουμε ότι ο πρώτος p εμφανίζεται στην ανάλυση του a με εκθέτη $e \geq 1$:

$$a = p^e \cdots$$

(ακολουθούν διαφορετικοί πρώτοι). Αν $a \mid b$ τότε $b = ka$, για κάποιο $k \in \mathbb{Z}$, οπότε

$$b = ka = kp^e \cdots$$

και άρα ο p εμφανίζεται στον b με εκθέτη τουλάχιστον e.

Η αντίστροφη κατεύθυνση είναι εξίσου φανερή αφού αν

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

και

$$b = p_1^{e_1'} p_2^{e_2'} \cdots p_k^{e_k'} p_{k+1}^{e_{k+1}'} \cdots p_r^{e_r'}$$

με $e_j' \geq e_j$, $j = 1, 2, \ldots, k$, τότε είναι προφανές ότι ο b είναι πολλαπλάσιο του a.
■

✏ **2.22**
Ας είναι $a, b \geq 1$ δύο ακέραιοι.

Δείξτε ότι στον (a, b) εμφανίζονται ακριβώς εκείνοι οι πρώτοι αριθμοί που εμφανίζονται και στον a και στον b και μάλιστα με εκθέτη ίσο με τον ελάχιστο εκθέτη που έχουν στους a, b.

Ομοίως δείξτε ότι στο $[a, b]$ εμφανίζονται ακριβώς εκείνοι οι πρώτοι αριθμοί που εμφανίζονται στον a ή στον b και μάλιστα με εκθέτη ίσο με το μέγιστο εκθέτη που έχουν στους a, b.

Γενικεύστε για περισσότερους από δύο ακεραίους.

💡 *Χρησιμοποιήστε το Λήμμα 2.2.*

✏ **2.23**
Αν $a, b \geq 1$ είναι ακέραιοι δείξτε ότι

$$(a, b)[a, b] = a \cdot b.$$

✏ **2.24**
Αν $a, b > 0$ είναι μεταξύ τους πρώτοι βρείτε τον $(a^2 + b^2, a + b)$.

✏ **2.25**
Αν a άρτιος και b περιττός δείξτε $(a, b) = (a/2, b)$. Αν και οι δύο είναι άρτιοι δείξτε $(a, b) = 2(a/2, b/2)$.

✏ **2.26**
Αν $(a, b) = 1$ και $c \mid a + b$ δείξτε $(c, a) = (c, b) = 1$.

✏ **2.27**
Αν α είναι ρίζα του πολυωνύμου

$$x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1 x + c_0,$$

όπου $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}$, δείξτε ότι αν το α δεν είναι ακέραιος τότε είναι άρρητος.

Δείξτε ότι οι αριθμοί $\sqrt{2}$, $\sqrt[3]{5}$, $\sqrt[10]{17}$ είναι άρρητοι.

💡 *Υποθέστε όχι και γράψτε $\alpha = \frac{k}{l}$ με $(k, l) = 1$ και $l > 1$. Ας είναι p κάποιος πρώτος διαιρέτης του l.*

✏ **2.28**
Βρείτε την ανάλυση του 4849845 σε γινόμενο πρώτων.

✏ **2.29**
Βρείτε όλους τους πρώτους που διαιρούν το 10!. Ομοίως για τον αριθμό $\binom{30}{10}$.

✏ **2.30**
Περιγράψτε όλους τους θετικούς ακεραίους που έχουν ακριβώς 3 διαιρέτες (συμπεριλαμβανομένου του 1 και τους εαυτού τους). Ομοίως για ακριβώς 4 διαιρέτες. Ομοίως για ακριβώς 5 διαιρέτες.

✏ **2.31**
Δείξτε ότι κάθε θετικός ακέραιος γράφεται σα γινόμενο ενός τέλειου τετραγώνου και ενός αριθμού ελεύθερου τετραγώνων (αυτοί είναι οι ακέραιοι πο υ δε διαιρούνται από το p^2 για κανένα πρώτο p).

✏ **2.32**
Δείξτε ότι η δύναμη με την οποία ο πρώτος p εμφανίζεται στο $n!$ είναι το άθροισμα

$$\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots .$$

Παρατηρήστε ότι το άθροισμα αυτό έχει πεπερασμένους σε πλήθος μη μηδενικούς όρους αφού για αρκετά μεγάλο j θα έχουμε $n/p^j < 1$.

Βρείτε την ανάλυση του 20! σε γινόμενο πρώτων.

Πόσα μηδενικά υπάρχουν στο τέλος του αριθμού 1000!; Πόσα αν τον ίδιο αριθμό τον γράψουμε στο 8-αδικό σύστημα;

✏ **2.33**
Ποια ζεύγη ακεραίων a, b έχουν μέγιστο κοινό διαιρέτη $(a, b) = 18$ και ελάχιστο κοινό πολλαπλάσιο $[a, b] = 240$;

✏ **2.34**
Δείξτε $c \mid ab \Longrightarrow c \mid (a, c)(b, c)$.

✏ **2.35**
Δείξτε $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.

✏ **2.36**
Δείξτε $\log_2 3 \notin \mathbb{Q}$.

✏ **2.37**
Δείξτε ότι ο αριθμός

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}$$

δεν είναι ποτέ ακέραιος αν $n \geq 2$.

✏ **2.38**
Δείξτε $(a, b) = (a + b, [a, b])$.

✏ **2.39**
Πόσα ζεύγη θετικών ακεραίων a, b υπάρχουν με $[a, b] = n$. Η απάντηση εξαρτάται από την ανάλυση του n σε πρώτους παράγοντες.

✏ **2.40**
Δείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $6k + 5$.

💡 *Δείξτε πρώτα ότι όλοι οι πρώτοι είναι της μορφής $6k+1$ ή $6k+5$. Υποθέστε ότι υπάρχουν πεπερασμένοι σε πλήθος πρώτοι της μορφής $6k + 5$, οι $p_1, p_2, \ldots, p_r$, και εξετάστε τον αριθμό $n = 6p_1p_2 \cdots p_r - 1$.*

✏ **2.41**
Αν πάρουμε ένα σύνολο από $n + 1$ διαφορετικούς ακεραίους από 1 έως $2n$ δείξτε ότι υπάρχει κάποιος στο σύνολο που διαιρεί κάποιον άλλο αριθμό του συνόλου.

Βιβλιογραφία Κεφαλαίου

[1] Ronald L Graham, Donald E Knuth, and Oren Patashnik. *Concrete Mathematics*. 1994.

[2] Godfrey Harold Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*. Oxford University Press, 1979.

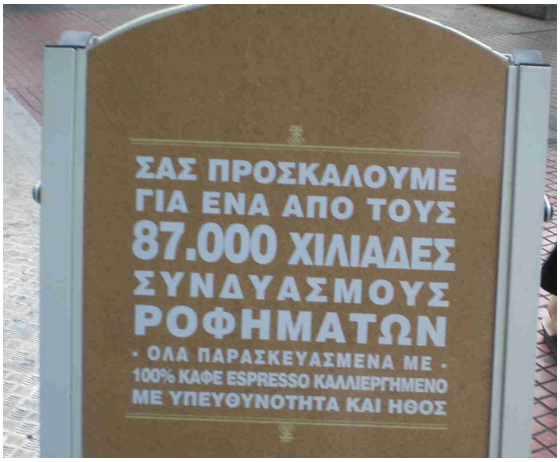
Κεφάλαιο 3

Βασικές αρχές απαρίθμησης

Κύριες βιβλιογραφικές αναφορές για αυτό το Κεφάλαιο είναι οι C. L. Liu and C. Liu 1985, Graham, Knuth, and Patashnik 1994, Cameron 1994 και Stanley 1986.

3.1 Αρχή πολλαπλασιασμού ανεξάρτητων επιλογών

Περπατώντας έξω από ένα κατάστημα που σερβίρει καφέδες διαφόρων ειδών συναντά κανείς τον ισχυρισμό που φαίνεται στο Σχήμα 3.1, που αρχικά φαίνεται μάλλον εξωφρενικός. Είναι όμως;



Σχήμα 3.1: Πόσους διαφορετικούς καφέδες μπορεί να φτιάξει ένα καφενείο;

Ας υποθέσουμε ότι κάποιος πίνει τον καφέ του με ή χωρίς ζάχαρη, με ή χωρίς γάλα. (Οι ποσότητες γάλατος και ζάχαρης που μπορεί κανείς να έχει είναι σταθερές. Δεν υπάρχει *με ολίγη*.) Πόσα διαφορετικά είδη από καφέ πρέπει να μπορεί να φτιαξει ένα καφενείο ώστε να μπορεί να εξυπηρετήσει όλους τους πελάτες;

Η απάντηση είναι 4:

1. Χωρίς γάλα, χωρίς ζάχαρη
2. Χωρίς γάλα, με ζάχαρη
3. Με γάλα, χωρίς ζάχαρη
4. Με γάλα, με ζάχαρη

Αν σκεφτούμε λίγο προσεκτικότερα θα συνειδητοποιήσουμε ότι $4 = 2 \cdot 2$ και ότι ο λόγος που η απάντηση είναι αυτή είναι ότι κάθε μια από τις δύο δυνατές επιλογές όσον αφορά το περιεχόμενο σε

γάλα μπορεί να συνδυαστεί με κάθε μία από τις δύο δυνατές επιλογές που αφορούν στο περιεχόμενο σε ζάχαρη.

✏ **3.1**
Ποια η απάντηση στο άνω «πρόβλημα του καφέ» αν οι επιλογές μας ως προς τη ζάχαρη δεν είναι πλέον οι ΝΑΙ, ΟΧΙ, αλλά μπορούμε είτε να μην έχουμε καθόλου ζάχαρη, είτε να έχουμε ένα φακελάκι, είτε δύο;

✏ **3.2**
Αν το αρχικό «πρόβλημα του καφέ» προστεθεί η επιλογή ΚΡΥΟΣ ή ΖΕΣΤΟΣ, την οποία μπορούμε να έχουμε ανεξάρτητα από το γάλα ή τη ζάχαρη που διαλέγουμε, ποια είναι η απάντηση;

Η αρχή του **πολλαπλασιασμού ανεξάρτητων επιλογών** κωδικοποιεί την απλή αυτή παρατήρηση που κάναμε:

> Ας υποθέσουμε ότι έχουμε να παραγματοποιήσουμε μια σύνθετη επιλογή, η οποία συνίσταται από την πραγματοποίηση k επί μέρους επιλογών, που πραγματοποιούνται *ανεξάρτητα* η μία από την άλλη, είναι δηλ. τέτοιες οι επί μέρους επιλογές ώστε η επιλογή τιμών για κάποιες από αυτές να μην επηρεάζει τις δυνατότητες που υπάρχουν για τις υπόλοιπες. Τότε το συνολικό πλήθος δυνατοτήτων που έχουμε για τη σύνθετή μας επιλογή είναι το γινόμενο των k δυνατοτήτων για τις επί μέρους επιλογές μας.

Σε πιο αυστηρή γλώσσα η αρχή του πολλαπλασιασμού ανεξαρτήτων επιλογών εκφράζεται ως εξής (γενικά με $|X|$ συμβολίζουμε τον πληθάριθμο–πόσα στοιχεία έχει–του συνόλου X):

Θεώρημα 3.1
Έστω k φυσικός αριθμός και E το σύνολο όλων των διαφορετικών k-άδων

$$(x_1, \ldots, x_k)$$

όπου $x_1 \in E_1, x_2 \in E_2, \ldots, x_k \in E_k$, και τα E_j είναι όλα πεπερασμένα σύνολα. Τότε

$$|E| = |E_1| \cdot |E_2| \cdots |E_k|.$$

Απόδειξη

Απόδειξη με επαγωγή ως προς k. Αν $k = 1$ πρόκειται περί ταυτολογίας, αφού $E = E_1$. Υποθέτουμε τώρα ότι η πρόταση ισχύει για $k = n$ και τη δείχνουμε για $k = n + 1$. Θέλουμε να μετρήσουμε τα διατεταγμένα αντικείμενα της μορφής

$$(x_1, \ldots, x_n, x_{n+1}) \tag{3.1}$$

όπου $x_j \in E_j$, για $j = 1, \ldots, n+1$. Αν $E_{n+1} = \{e_1, \ldots, e_r\}$ αυτά τα αντικείμενα (3.1) χωρίζονται στις εξής *ξένες* μεταξύ τους r ομάδες: G_1 είναι εκείνα τα αντικείμενα που στην τελευταία θέση τους έχουν e_1, δηλ. όλα τα αντικείμενα της μορφής

$$(x_1, \ldots, x_n, e_1),\ \mu\epsilon\ x_j \in E_j, \tag{3.2}$$

G_2 είναι εκείνα τα αντικείμενα με e_2 στην τελευταία θέση, κ.ο.κ. Οι ομάδες αυτές είναι μεταξύ τους ισοπληθείς, αφού, π.χ. μπορεί η G_1 να τεθεί σε 1-1 και επί αντιστοιχία με τη G_2 μέση της απεικόνισης $G_1 \to G_2$

$$(x_1, \ldots, x_n, e_1) \to (x_1, \ldots, x_n, e_2).$$

Το συνολικό πλήθος λοιπόν των αντικειμένων τύπου (3.1) είναι

$$|G_1| \cdot r = |G_1| \cdot |E_{n+1}|. \tag{3.3}$$

Αλλά, είναι φανερό, το πλήθος στοιχείων της G_1 είναι όσα και τα διατεταγμένα αντικείμενα

$$(x_1, \ldots, x_n),\ \mu\epsilon\ x_j \in E_j,$$

που, λόγω της επαγωγικής υπόθεσης, είναι ίσο με $|E_1| \cdots |E_n|$. Αντικαθιστώντας στην (3.3) παίρνουμε το αποτέλεσμα.
■

✏ **3.3**

Το παρακάτω πρόγραμμα σε python υπολογίζει όλα τα ζεύγη (x, y) όπου $x \in A, y \in B$, όλα τα στοιχεία δηλ. του καρτεσιανού γινομένου $A \times B$.

```
A = ['Sweet', 'Medium', 'No Sugar']
B = ['With milk', 'No milk']
for x in A:
    for y in B:
        print "Sugar: ", x, " Milk: ", y
```

Τρέξτε το πρόγραμμα. Πόσες γραμμές τυπώνει; Τροποποιήστε το πρόγραμμα ώστε να συμπεριλαμβάνει και ένα επιπλέον χαρακτηριστικό του καφέ, το μέγεθος, το οποίο έχει τρεις δυνατές τιμές:

```
C = ['Large', 'Medium', 'Small']
```

✏ **3.4**

Σε μια χώρα οι τηλεφωνικοί αριθμοί είναι όλοι δεκαψήφιοι. Το πρώτο ψηφίο κάθε τηλεφωνικού αριθμού μπορεί να είναι 2 ή 3 μόνο. Δεν υπάρχει περιορισμός για τα άλλα 9 ψηφία. Ποιος είναι ο μέγιστος αριθμός τηλεφώνων που μπορεί να υπάρξει ταυτόχρονα σε αυτή τη χώρα;

✏ **3.5**

Πόσους δεκαδικούς ακεραίους με το πολύ τρία ψηφία μπορεί κανείς να γράψει χρησιμοποιώντας μόνο τα γράμματα 2,3,5;

Πόσους μονοψήφιους, πόσους διψήφιους και πόσους τριψήφιους μπορείτε να φτιάξετε;

✏ **3.6**

Πόσες διαφορετικές στήλες ΠΡΟ-ΠΟ υπάρχουν (μήκους 14, με 1,2 ή X σε κάθε θέση);

✏ **3.7**

Πόσες διαφορετικές τριάδες γραμμάτων μπορούν να εμφανιστούν σε ελληνικές πινακίδες αυτοκινήτων; (Σε αυτές χρησιμοποιούνται μόνο γράμματα που ανήκουν και στο ελληνικό και στο λατινικό αλφάβητο. Αυτά τα γράμματα είναι 14 τον αριθμό.) Αν κάθε τέτοια τριάδα ακολουθείται από ένα τετραψήφιο φυσικό αριθμό (με πρώτο ψηφίο διαφορετικό από το 0) πόσα το πολύ αυτοκίνητα μπορούν να ταξινομηθούν στην Ελλάδα;

Λύστε το ίδιο πρόβλημα για πινακίδες μοτοσυκλετών: 3 γράμματα ακολουθούμενα από ένα αριθμό που μπορεί να είναι μονοψήφιος, διψήφιος ή τριψήφιος αλλά όχι 0.

✏ **3.8**

Αν ρίχνετε συνεχώς ένα ζευγάρι τίμια ζάρια, πόσο συχνά περιμένετε να φέρετε δύο άσους; Άσο και δύο;

Εμμέσως υποθέτουμε εδώ ότι όλα τα δυνατά αποτελέσματα αυτού του πειράματος είναι εξίσου πιθανά. Αν είναι λοιπόν N ο αριθμός όλων των δυνατών αποτελεσμάτων τότε το κάθε ένα από αυτά εμφανίζεται περίπου το $1/N$ του χρόνου (με συχνότητα δηλ. $1/N$). Πρώτα λοιπόν θα πρέπει να βρείτε το N: πόσα είναι τα δυνατά αποτελέσματα αυτού του πειράματος; Πόσα είναι δηλ. τα δυνατά ζεύγη (x, y), με

$$x, y \in \{1, 2, 3, 4, 5, 6\};$$

Εδώ x συμβολίζει την ένδειξη του πρώτου ζαριού και y συμβολίζει την ένδειξη του δεύτερου ζαριού. Προσέξτε μόνο ότι το δεύτερο ερώτημα αντιστοιχεί σε δύο τέτοια ζεύγη και όχι μόνο σε ένα όπως το πρώτο ερώτημα.

3.1.1 Πλήθος υποσυνόλων ενός πεπερασμένου συνόλου

Η πρώτη σημαντική εφαρμογή της αρχής πολλαπλασιασμού των ανεξάρτητων επιλογών είναι το ακόλουθο.

Θεώρημα 3.2
Έστω σύνολο A με n στοιχεία, και $\mathcal{P}(A)$ το δυναμοσύνολο *του A, δηλ. το σύνολο όλων των υποσυνόλων του A. Τότε*

$$|\mathcal{P}(A)| = 2^n.$$

Απόδειξη

Μπορεί κανείς εύκολα να αποδείξει το Θεώρημα με επαγωγή ως προς το n, αλλά ας δούμε πώς αποδεικνύεται εφαρμόζοντας την αρχή πολλαπλασιασμού. Η βασική παρατήρηση είναι ότι το πλήθος όλων των υποσυνόλων του $A = \{a_1, \ldots, a_n\}$ μπορεί να τεθεί σε 1-1 και επί αντιστοιχία με το σύνολο όλων των διατεταγμένων n-άδων

$$(x_1, \ldots, x_n) \ \mu\epsilon \ x_1, \ldots, x_n \in \{0, 1\}. \tag{3.4}$$

Όντως, η 1-1 και επί αυτή αντιστοιχία είναι αυτή που στέλνει το τυχόν υποσύνολο $B \subseteq A$ στη n-άδα $(x_1, \ldots, x_n)$ όπου $x_j = 1$ αν και μόνο αν $j \in B$ (βεβαιωθείτε ότι αυτή η απεικόνιση όντως είναι 1-1 και επί).

Αντί να μετρήσουμε λοιπόν τα στοιχεία του

$$\mathcal{P}(A) = \{B : \ B \subseteq A\}$$

μπορούμε να μετρήσουμε το πλήθος των n-άδων (3.4). Το αποτέλεσμα είναι το ίδιο.

Για να μετρήσουμε τώρα τις n-άδες (3.4) σκεφτόμαστε ως εξής: για να επιλέξουμε μια τυχούσα n-άδα πρέπει να κάνουμε n ανεξάρτητες επιλογές, μια για κάθε x_j, και σε κάθε μια από αυτές τις επιλογές έχουμε δύο δυνατότητες. Άρα, το πλήθος δυνατοτήτων για τη συνολική επιλογή είναι $\underbrace{2 \cdot 2 \cdots 2}_{n} = 2^n$.

■

✏ **3.9**
Δώστε επαγωγική απόδειξη (ως προς το n) του Θεωρήματος 3.2.

✏ **3.10**
Το παρακάτω πρόγραμμα σε python υπολογίζει το δυναμοσύνολο ενός συνόλου. Το σύνολο το αναπαριστάμε με μια λίστα (που φροντίζουμε να μην έχει στοιχεία που επαναλαμβάνονται).

```
def subsets(s):
    n = len(s)
    # empty set contains only the empty set
    if n==0:
        return [[]]
    # s1 is set s without its first element
    s1 = s[1:]
    f = s[0] # f is the first element of set s
    # all subsets of s not containing its first element, f
    p1 = subsets(s1)
    # p2 will contain all subsets of s containing f
    p2 = []
    for x in p1:
        p2.append([f]+x)
    return p2+p1
```

Κατανοήστε το πώς δουλεύει αυτή η συνάρτηση `subsets`. *(Η συνάρτηση αυτή είναι αναδρομική (recursive), καλεί δηλ. τον εαυτό της.) Μπορείτε να τη δοκιμάσετε ως εξής:*

```
s = ['a', 'b', 'c', 'd']
print subsets(s)
```

για να πάρετε το output

```
[['a', 'b', 'c', 'd'], ['a', 'b', 'c'], ['a', 'b', 'd'],
 ['a', 'b'], ['a', 'c', 'd'], ['a', 'c'], ['a', 'd'], ['a'],
 ['b', 'c', 'd'], ['b', 'c'], ['b', 'd'],
 ['b'], ['c', 'd'], ['c'], ['d'], []]
```

Παράδειγμα 3.1
Μέ πόσους τρόπους μπορεί κανείς να επιλέξει δύο ξένα μεταξύ τους υποσύνολα A και B του συνόλου $[n] = \{1, 2, \ldots, n\}$;

Τα σύνολα αυτά μπορούν να είναι και κενά.

Για να απαντήσουμε σκεφτόμαστε ως εξής, και ο τρόπος αυτός σκέψης αποτελεί υπόδειγμα για το πώς σκεφτόμαστε στην πλειονότητα των περιπτώσεων. Για να μετρήσουμε λοιπόν τα συγκεκριμένα αντικείμενα βρίσκουμε, κατ' αρχήν, μια διαδικασία για να τα κατασκευάσουμε. Αυτή η διαδικασία πρέπει να είναι τέτοια ώστε

- *Να κωδικοποιείται με μια ακολουθία από επιλογές μετά από τις οποίες καταλήγουμε σε ένα από τα αντικείμενα της κλάσης που προσπαθούμε να μετρήσουμε,*
- *Για κάθε μια από τις δυνατές ακολουθίες επιλογών που κάνουμε να προκύπτει και ένα διαφορετικό αντικείμενο από την κλάση, και*
- *Για κάθε στοιχείο της κλάσης των προς μέτρηση αντικειμένων υπάρχει μια ακολουθία επιλογών (που είναι και μοναδική, από την προηγούμενη απαίτηση) που μας δίνει το στοιχείο αυτό.*

Η κατασκευή που δίνουμε για το συγκεκριμένο πρόβλημα είναι η εξής. Προχωράμε για $i = 1$ έως $i = n$ και για κάθε i επιλέγουμε αν θα είναι στο σύνολο A, στο σύνολο B ή αν δε θα είναι σε κανένα από αυτά. Δε μπορεί να είναι και στα δύο αφού τα A και B τα θέλουμε ξένα μεταξύ τους. (Δείτε Σχήμα 3.2.)

Σχήμα 3.2: Τοποθετούμε κάθε ένα από τα $1, 2, \ldots, n$ σε ακριβώς ένα από τα τρία σακιά

Είναι φανερό πως αν έχουμε δύο διαφορετικές ακολουθίες από τις n αυτές επιλογές, τότε αυτές οδηγούν σε δύο διαφορετικά αντικείμενα, σε δύο διαφορετικά δηλ. ζεύγη ξένων υποσυνόλων $A, B \subseteq [n]$. Έτσι, το πλήθος των αντικειμένων που μας ενδιαφέρει είναι ίσο με το πλήθος των δυνατών ακολουθιών επιλογών μας. Είναι επίσης φανερό ότι οι n απλές επιλογές που απαρτίζουν αυτή την ακολουθία επιλογών είναι ανεξάρτητες μεταξύ τους, αφού κάθε φορά, και ότι και να έχουμε επιλέξει μέχρι στιγμής, τρείς είναι οι δυνατές επιλογές μας για τον τρέχοντα αριθμό i, δηλ. να επιλέξουμε $i \in A$, $i \in B$ ή $i \notin A \cup B$. Έτσι, το τελικό αποτέλεσμα είναι

$$\underbrace{3 \cdots 3}_{n} = 3^n.$$

✏ **3.11**
Με πόσους τρόπους μπορούμε να επιλέξουμε δύο υποσύνολα A και B του $[n]$ ώστε $A \subseteq B$;

Σχήμα 3.3: Τα σακιά που πρέπει να χρησιμοποιήσετε για την Άσκηση 3.11

✏ **3.12**
Ποια η απάντηση στο ερώτημα του Παραδείγματος 3.1 αν απαιτήσουμε τα σύνολα A και B να είναι μη κενά;
Αφαιρέστε από την απάντηση που δόθηκε στο Παράδειγμα 3.1 μια κατάλληλη ποσότητα που αντιπροσωπεύει επιλογές που δεν πληρούν το κριτήριο της μη κενότητας που έχουμε θέσει.

3.1.2 Πλήθος συναρτήσεων από σύνολο A σε σύνολο B

Μια συνάρτηση από το σύνολο A στο σύνολο B είναι απλά μια αντιστοίχιση *κάθε* στοιχείου του A σε *κάποιο* στοιχείο του B. Αν $|A| = m$ και $|B| = n$ πόσες τέτοιες συναρτήσεις υπάρχουν; Η απάντηση είναι n^m:

Θεώρημα 3.3
Αν A και B είναι δύο πεπερασμένα σύνολα, και με B^A συμβολίσουμε το σύνολο όλων των συναρτήσεων από το A στο B, τότε

$$\left|B^A\right| = |B|^{|A|}.$$

Απόδειξη

Το να επιλέξουμε μια συνάρτηση από το A στο B (ένα μέλος δηλ. του συνόλου B^A) σημαίνει απλούστατα να επιλέξουμε την εικόνα κάθε στοιχείου του A ανάμεσα σε όλα τα στοιχεία του B. Οι επιλογές αυτές είναι προφανώς ανεξάρτητες μεταξύ τους αφού δεν έχουμε θέσει κανένα περιορισμό στο τι είδους συναρτήσεις θέλουμε (π.χ., θα μπορούσαμε να θέλουμε 1-1 συναρτήσεις μόνο–σε αυτή την περίπτωση οι επιλογές δε θα ήταν φυσικά ανεξάρτητες). Έτσι το πλήθος των δυνατών επιλογών είναι

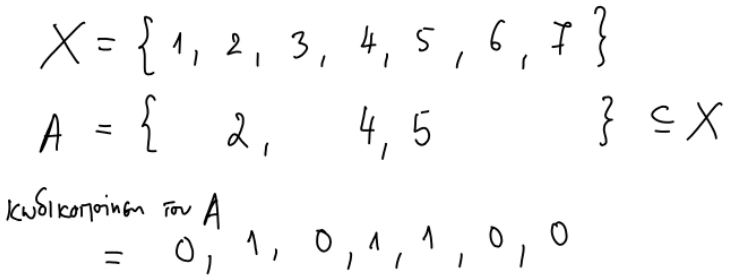
$$\underbrace{|B| \cdots |B|}_{|A|} = |B|^{|A|}.$$

■

✏ **3.13**
Ποιο το πλήθος των συναρτήσεων $[n] \to \{0, 1\}$; (Περιγράψτε μια φυσιολογική σχέση με τα υποσύνολα του $[n]$.)

✏ **3.14**
Πόσοι $m \times n$ πίνακες υπάρχουν με στοιχεία 0, 1 ή 3;

✏ **3.15**
Ποιο το πλήθος των συναρτήσεων $f : [n] \to \mathbb{N} = \{0, 1, 2, \ldots\}$ που πληρούν την ανισότητα $f(k) < k$ για κάθε $k \in [n]$;
Πόσες επιλογές έχετε για την εικόνα του k;



Σχήμα 3.4: Μια κωδικοποίηση υποσυνόλων του X με μια απεικόνιση $X \to \{0,1\}$, για την Άσκηση 3.13

✏ **3.16**
Αν $A = \{-n, -n+1, \ldots, n-1, n\}$ ποιο το πλήθος των συναρτήσεων $A \to A$ που είναι άρτιες, πληρούν δηλ. $f(-x) = f(x)$ για όλα τα $x \in A$;

✏ **3.17**
Πόσοι μη αρνητικοί ακέραιοι αριθμοί, μικρότεροι από 10^6, έχουν κάποιο 2 στο δεκαδικό τους ανάπτυγμα;
Πόσοι δεν *έχουν;*

✏ **3.18**
Πόσους διαιρέτες έχει ο φυσικός αριθμός

$$n = p_1^{\nu_1} \cdots p_k^{\nu_k}; \tag{3.5}$$

*Ο n έχει γραφεί σαν γινόμενο δυνάμεων ξένων μεταξύ τους πρώτων αριθμών p_j. (*Πρώτος *λέγεται ένας ακέραιος μεγαλύτερος του 1 αν δεν έχει άλλους διαιρέτες παρά μόνο τον εαυτό του και το 1. Π.χ. πρώτοι αριθμοί είναι οι 2, 3, 5, 7, 11, 13, ενώ ο 6 δεν είναι πρώτος, αλλά* σύνθετος *αριθμός. Υπάρχουν άπειροι πρώτοι αριθμοί.) Μπορείτε να χρησιμοποιήσετε το θεμελιώδες θεώρημα (Θεώρημα 2.6) που λέει ότι κάθε φυσικός αριθμός n γράφεται κατά μοναδικό τρόπο στη μορφή (3.5), εκτός ίσως από τη σειρά των παραγόντων.*

Εφαρμόστε το αποτέλεσμά σας στον αριθμό 100 και απαριθμήστε και τους διαιρέτες του έναν-έναν μαζί με το ανάπτυγμα του καθενός σε γινόμενο πρώτων.

3.2 Αρχή πολλαπλασιασμού ημι-ανεξάρτητων επιλογών

Είδαμε στην §3.1 ότι όταν έχουμε να παραγματοποιήσουμε μια σύνθετη επιλογή που αποτελείται από πολλές επί μέρους επιλογές, οι οποίες είναι ανεξάρτητες η μια από την άλλη, μπορούμε δηλ. να πραγματοποιήσουμε τις επί μέρους επιλογές όλες ταυτόχρονα, τότε το πλήθος δυνατοτήτων για τη σύνθετη επιλογή ισούται με το γινόμενο των δυανατοτήτων για τις επί μέρους επιλογές.

Η αρχή πολλαπλασιασμού γίνεται πολύ χρησιμότερη μετά από την εξής παρατήρηση. Δε χρειάζεται οι επί μέρους επιλογές μας να είναι ανεξάρτητες. Μπορούμε να επιτρέψουμε η πρώτη μας επί μέρους επιλογή να επηρεάζει τις δυνατότητές μας για τη δεύτερη (ή κάποια άλλη) επιλογή, αρκεί να μην επηρεάζει το *πλήθος* των δυνατοτήτων για την επιλογή αυτή. Δεν απαιτούμε δηλ. να μένει το σύνολο δυνατοτήτων της κάθε επί μέρους επιλογής αναλλοίωτο από κάθε προηγούμενή μας απόφαση, αρκεί να μένει το μέγεθος του συνόλου αναλλοίωτο. Λέμε τότε ότι οι επί μέρους επιλογές μας είναι *ημι-ανεξάρτητες* (ο όρος δεν είναι καθιερωμένος).

Παράδειγμα 3.2
Ας υποθέσουμε ότι, παράλληλα με τις υποθέσεις της Άσκησης 3.1, σε ένα περιέργο τόπο ο κόσμος δεν πίνει ποτέ σκέτο καφέ χωρίς γάλα και ότι δεν πίνει επίσης ποτέ γλυκό (2 φακελάκια ζάχαρη) με γάλα. Το πλήθος των δυνατών τύπων καφέ είναι πάλι $2 \cdot 2$ αν και τώρα οι επιλογές (γάλα, ζάχαρη) δεν είναι πλέον

ανεξάρτητες, αφού αν κάποιος επιλέξει πρώτα καφέ χωρίς γάλα οι επιλογές του ως προς τη ζάχαρη είναι 1 ή 2 φακελάκια ενώ αν επιλέξει καφέ με γάλα οι επιλογές του ως προς τη ζάχαρη είναι 0 ή 1 φακελάκι. Οι επιλογή δηλ. που κάνουμε για το γάλα επηρεάζει τις επιλογές μας για τη ζάχαρη, αλλά όχι το πλήθος των επιλογών αυτών, είναι δηλ. η επιλογή της ζάχαρης ημιανεξάρτητη από την επιλογή του γάλακτος.

Παρατήρηση 3.1
Είναι πάρα πολύ σημαντικό να παρατηρήσουμε εδώ ότι η έννοια της ημι-ανεξαρτησίας όπως την ορίσαμε περιγραφικά εδώ εξαρτάται *από τη σειρά με την οποία πραγματοποιούνται οι επί μέρους επιλογές. Αν στο Παράδειγμα 3.2 επιλέξει κανείς πρώτα το επίπεδο ζάχαρης και μετά το αν θα έχει ο καφές του γάλα ή όχι, παύει η ημι-ανεξαρτησία. Αν επιλέξει κάποιος ο καφές του να είναι σκέτος (καθόλου ζάχαρη) τότε έχει μία επιλογή για το γάλα: πρέπει οπωσδήποτε να βάλει. Αν επιλέξει 1 φακελάκι ζάχαρη μπορεί βάλει γάλα ή όχι, ενώ αν επιλέξει 2 φακελάκια ζάχαρη πάλι έχει 1 επιλογή: να μη βάλει γάλα. Αν αθροίσουμε το πλήθος των επιλογών τότε παίρνουμε πάλι $1+2+1=4$ φυσικά. Αλλά παρατηρήστε ότι αυτός ο τρόπος μετρήματος είναι πιο περίπλοκος μια και δεν μπορούμε πλέον να πολλαπλασιάσουμε τις επιλογές, αλλά πρέπει να αθροίσουμε. Γι' αυτό και ένα μεγάλο κομμάτι από την τέχνη του μετρήματος έγκειται στο να διαλέξουμε μια καλή σειρά μετρήματος, που θα οδηγήσει σε απλό μέτρημα.*

Παράδειγμα 3.3
Μια 10-μελής ομάδα επιλέγει αρχηγό και (διαφορετικό) υπαρχηγό. Με πόσους τρόπους μπορεί να γίνει αυτό;

Η απάντηση είναι με $10 \cdot 9 = 90$ διαφορετικούς τρόπους. Πρώτα επιλέγεται ο αρχηγός και μετά ο υπαρχηγός. Για τον αρχηγό έχουμε 10 επιλογές. Αφού επιλεγεί αυτός, έστω ο x, στη θέση του υπαρχηγού μπορούμε να επιλέξουμε οποιονδήποτε εκτός του x, έχουμε δηλ. 9 επιλογές. Παρατηρήστε ότι οι δύο επιλογές δεν είναι ανεξάρτητες αφού η επιλογή του αρχηγού επηρεάζει το σύνολο των δυνατών επιλογών για υπαρχηγό, δεν επηρεάζει όμως το πλήθος των δυνατών υπαρχηγών. Είναι δηλ. οι δύο αυτές επιλογές ημι-ανεξάρτητες.

✏ **3.19**
Έστω μια ομάδα 5 ανδρών και μια ομάδα 7 γυναικών. Με πόσους τρόπους μπορούμε να παντρέψουμε και τους 5 άνδρες με γυναίκες από αυτή την ομάδα των 7; Ισχύουν οι συνήθεις κανόνες (όχι διγαμία).

✏ **3.20**
Για $m \leq n$ πόσες 1-1 συναρτήσεις υπάρχουν από το $[m]$ στο $[n]$;
Επιλέγετε την εικόνα των $1, 2, \ldots, m$ με τη σειρά. Έχοντας επιλέξει τις εικόνες των $1, 2, \ldots, k-1$ πόσες επιλογές έχετε για την εικόνα του k;

✏ **3.21**
Στην Άσκηση 3.19 αλλάξτε τους κοινωνικούς κανόνες ώστε να επιτρέπουν σε μια γυναίκα να παντρευτεί ταυτόχρονα όσους άντρες θέλει. Και πάλι πρέπει να παντρευτούν όλοι οι άντρες και ο ίδιος άντρας δε μπορεί να είναι παντρεμένος με δύο γυναίκες.

3.2.1 Πλήθος διατεταγμένων επιλογών. Μεταθέσεις συνόλου

Με πόσους τρόπους μπορούμε να διαλέξουμε, κατά τρόπο διατεταγμένο, r άτομα από n;

Θεώρημα 3.4
Το πλήθος των διατεταγμένων r-άδων ($r \leq n$)

$$(x_1, \ldots, x_r), \tag{3.6}$$

με $x_j \in [n]$ όλα διαφορετικά, είναι

$$n(n-1)(n-2)\cdots(n-r+1).$$

Απόδειξη

Επιλέγουμε πρώτα το x_1. Γι' αυτό έχουμε n δυνατότητες. Έχοντας επιλέξει το x_1 δεν μπορούμε πλέον να διαλέξουμε το ίδιο στοιχείο και για x_2. Οι δυνατότητες που έχουμε άρα για το x_2 είναι μία λιγότερες, δηλ. $n-1$. Έχοντας επιλέξει τα x_1, x_2 οι δυνατότητες για το x_3 είναι πλέον $n-2$, κλπ. Παρατηρούμε ότι οι επιλογές είναι ημι-ανεξάρτητες. Δεν επηρεάζουν δηλ. οι μέχρι κάποια στιγμή επιλογές μας το *πλήθος* των μετέπειτα επιλογών μας. Εφαρμόζοντας την αρχή του πολλαπλασιασμού παίρνουμε το αποτέλεσμα, αφού για το x_r θα έχουμε $n - r + 1 = n - (r - 1)$ δυνατότητες αφού θα έχουν ήδη χρησιμοποιηθεί ακριβώς $r - 1$ στοιχεία από τα n.
■

Πόρισμα 3.1
Το πλήθος των τρόπων να διατάξουμε στη σειρά τα στοιχεία ενός συνόλου με n στοιχεία είναι

$$n! = 1 \cdot 2 \cdot 3 \cdots n.$$

Οι διαφορετικοί αυτοί τρόποι διάταξης όλων των στοιχείων ενός συνόλου λέγονται μεταθέσεις *του συνόλου.*

Απόδειξη

Το να διατάξουμε τα στοιχεία του συνόλου στη σειρά είναι το ίδιο πράγμα με το να διαλέξουμε μια διατεταγμένη n-άδα από αυτά. Εφαρμόζουμε λοιπόν το Θεώρημα 3.4 με $r = n$.
■

✏ **3.22**

Το παρακάτω πρόγραμμα σε python βρίσκει όλες τις μεταθέσεις ενός συνόλου (το οποίο, ως συνήθως, αναπαριστούμε ως μια λίστα με διαφορετικά στοιχεία).

```
def permutations(s):
    """
    Returns a list of all perumatations of the set (list) s.
    Each element of this list is a permutation of s (again, a list).
    The list s is assumed to be nonempty.
    """
    n = len(s)
    if n==1:
        return [s] # One permutation only
    else:
        result = [] # we will return this variable
        for x in s: # list all permutations of s with first element x
            ss = s[:] # make a copy of s
            ss.remove(x) # now ss is the original list with x removed
            for l in permutations(ss):
                result.append([x] + l) # we add each of them to result
        return result
```

Μπορείτε π.χ. να καλέσετε τη συνάρτηση δίνοντας

```
print permutations(['a', 'b', 'c', 'd'])
```

οπότε θα πάρετε το output

```
[['a', 'b', 'c', 'd'], ['a', 'b', 'd', 'c'],
['a', 'c', 'b', 'd'], ['a', 'c', 'd', 'b'],
['a', 'd', 'b', 'c'], ['a', 'd', 'c', 'b'],
['b', 'a', 'c', 'd'], ['b', 'a', 'd', 'c'],
['b', 'c', 'a', 'd'], ['b', 'c', 'd', 'a'],
```

```
['b', 'd', 'a', 'c'], ['b', 'd', 'c', 'a'],
['c', 'a', 'b', 'd'], ['c', 'a', 'd', 'b'],
['c', 'b', 'a', 'd'], ['c', 'b', 'd', 'a'],
['c', 'd', 'a', 'b'], ['c', 'd', 'b', 'a'],
['d', 'a', 'b', 'c'], ['d', 'a', 'c', 'b'],
['d', 'b', 'a', 'c'], ['d', 'b', 'c', 'a'],
['d', 'c', 'a', 'b'], ['d', 'c', 'b', 'a']]
```

Το πρόγραμμα είναι αναδρομικό (recursive). Βεβαιωθείτε ότι καταλαβαίνετε πώς δουλεύει.

✏ 3.23

Γράψτε ένα πρόγραμμα στη γλώσσα python που να υπολογίζει το παραγοντικό του n, το οποίο το δίνει ο χρήστης. Προσέξτε ότι το n θα πρέπει να είναι ακέραιος και ότι για $n < 0$ το παραγοντικό δεν ορίζεται (το πρόγραμμα θα πρέπει να τυπώνει κάποιο μήνυμα σε αυτή την περίπτωση). Επίσης προσέξτε ότι $0! = 1$.

Γράψτε το πρόγραμμά σας συμπληρώνοντας τα κενά στον παρακάτω κώδικα:

```
def factorial(n):
    # n should be >= 0
    if n<0:
        ............
    else:
        t=1
        ............
        return t
```

Έχοντας γράψει τη συνάρτησή σας μπορείτε να την ελέγξετε με την εντολή π.χ.

```
print factorial(5)
```

✏ 3.24

Γράψτε όλες τις μεταθέσεις του συνόλου $\{A, B, C\}$.

Μπορείτε αν θέλετε να χρησιμοποιήσετε το πρόγραμμα της Άσκησης 3.22.

✏ 3.25

Με πόσους τρόπους μπορούν να διαταχθούν τα ψηφία 1,2,3,4,5; Με πόσους τα ψηφία 1,1,3,4,5;

Για το δεύτερο ερώτημα βρείτε πρώτα με πόσους τρόπους μπορούν να μπουν στη σειρά τα σύμβολα 1, 1', 3, 4, 5. Με ποια διαδικασία μπορείτε να πάρετε από αυτούς τους τρόπους όλους τους τρόπους διάταξης των 1, 1, 3, 4, 5;

Με πόσους τρόπους μπορείτε να διατάξετε τα ψηφία 1, 1, 1, 2, 2, 3, 4, 5;

✏ 3.26

Σε μια πόλη με εξαψήφια τηλέφωνα πόσα νούμερα το πολύ μπορεί να υπάρχουν χωρίς επαναλαμβανόμενα ψηφία;

✏ 3.27

Ένα μήνυμα στον κώδικα Morse είναι μια πεπερασμένη ακολουθία (μια λέξη όπως λέμε) από κουκίδες, παύλες και κενά. Πόσα διαφορετικά μηνύματα φτιάχνονται με 7 κουκίδες, 3 παύλες και 2 κενά.

Πόσα αν απαγορεύεται ένα μήνυμα να ξεκινάει ή να τελειώνει με κενό;

✏ 3.28

Η νεοσύστατη εταιρεία πληροφορικής «Faster Than Light» ετοιμάζεται να φτιάξει ένα σύστημα για online email το οποίο φιλοδοξεί να καλύψει στο μέλλον πάνω από 100 εκατομμύρια χρήστες. Η εταιρεία έχει αποφασίσει ότι όλες οι διευθύνσεις email των χρηστών της θα είναι της μορφής

username`@does-not-get-there.ever`

όπου το username του χρήστη θα απαρτίζεται από το πολύ N γράμματα από το σύνολο

`A, B, C, D, …, Z, 0, 1, …, 9`

(36 σύμβολα συνολικά) με τον περιορισμό ότι το πρώτο γράμμα του username *πρέπει να είναι γράμμα και όχι αριθμός. (Τα κεφαλαία γράμματα ταυτίζονται με τα μικρά.) Ποια είναι η ελάχιστη τιμή του N που πρέπει να προβλέψει η εταιρεία ώστε να μπορεί να ικανοποιήσει το στόχο της και να έχει τουλάχιστον 100 εκατομμύρια διαθέσιμες διευθύνσεις στην αρχή της λειτουργίας της;*

✏ **3.29**
Αποδείξτε ότι $\frac{n!}{2^n} \to \infty$, για $n \to \infty$.

3.2.2 Μη διατεταγμένες επιλογές. Συνδυασμοί

Πόσα υποσύνολα του συνόλου $[n]$ (ή, εν γένει, ενός συνόλου με n στοιχεία) υπάρχουν με μέγεθος k;

Θεώρημα 3.5
Αν $0 \leq k \leq n$ τότε το σύνολο $[n]$ (ή οποιοδήποτε σύνολο με n στοιχεία) έχει

$$\binom{n}{k} := \frac{n(n-1)\cdots(n-k+1)}{k!}$$

υποσύνολα μεγέθους k (ακολουθούμε τη σύμβαση ότι ένα γινόμενο με 0 παράγοντες ισούται με 1, έτσι $0! = 1$).

Το σύμβολο $\binom{n}{k}$ προφέρεται: n ανά k.

Πόρισμα 3.2
Αν n, k φυσικοί αριθμοί, $0 \leq k \leq n$, τότε α αριθμός

$$\frac{n(n-1)\cdots(n-k+1)}{k!}$$

είναι ακέραιος.

Απόδειξη

Αυτό που ζητάμε να μετρήσουμε είναι το πλήθος των μη διατεταγμένων k-άδων με διαφορετικά στοιχεία από το $[n]$. Λέγοντας ότι θέλουμε να μετρήσουμε «μη διατεταγμένες» k-άδες εννούμε ότι αν δύο k-άδες διαφέρουν μόνο ως προς τη σειρά που εμφανίζονται τα στοιχεία τους, τότε αυτές τις θεωρούμε ίδιες και τις μετράμε μία φορά. Αν αυτό δεν ίσχυε, αν δηλ. διαφορετικά διατεταγμένες k-άδες θεωρούνταν διαφορετικές, τότε την απάντηση τη δίνει το Θεώρημα 3.4, δηλ. $n(n-1)\cdots(n-k+1)$.

Παρατηρήστε τώρα ότι σε κάθε μη διατεταγμένη k-άδα, σε κάθε δηλ. k-μελές υποσύνολο του $[n]$, αντιστοιχούν ακριβώς $k!$ διατεταγμένες k-άδες, μια και με τόσους τρόπους μπορούν να διαταχθούν τα στοιχεία ενός k-μελούς συνόλου (Πόρισμα 3.1). Άρα, στον αριθμό $n(n-1)\cdots(n-k+1)$ κάθε k-μελές υποσύνολο του $[n]$ έχει μετρηθεί ακριβώς $k!$ φορές. Για να βρούμε συνεπώς το πλήθος των k-μελών υποσυνόλων του $[n]$ αρκεί να διαιρέσουμε αυτό τον αριθμό με $k!$.
■

Παρατήρηση 3.2
Είναι σημαντικό να τονίσουμε εδώ ότι η προηγούμενη απόδειξη δουλεύει ακριβώς επειδή κάθε k-μελές σύνολο είχε μετρηθεί τον ίδιο αριθμό φορών *στην ποσότητα $n(n-1)\cdots(n-k+1)$, και άρα δικαιούμασταν να διαιρέσουμε δια αυτό τον αριθμό φορών.*

✏ **3.30**
Το παρακάτω πρόγραμμα σε python υπολογίζει το διωνυμικό συντελεστή $\binom{n}{k}$ και τυπώνει για δοκιμή την τιμή $\binom{5}{2}$:

```
def binomial(n,k):
    if k<0:
        print "Error"
        return -1
    else:
        t=1.0
        for i in range(k):
            t = t*(n-i)/(k-i)
        return t

print binomial(5,2)
```

Βεβαιωθείτε ότι καταλαβαίνετε τον τρόπο λειτουργίας του και τρέξτε μερικά παραδείγματα. Παρατηρήστε ότι αν στη θέση του n βάλουμε έναν οποιοδήποτε πραγματικό αριθμό το πρόγραμμα τρέχει κανονικά αλλά προκύπτει σφάλμα αν στη θέση του k βάλουμε κάποιον αριθμό που δεν είναι φυσικός αριθμός.

Στην πραγματικότητα το πρόγραμμα αυτό υπολογίζει το πολυώνυμο

$$\binom{x}{k} = \frac{x(x-1)(x-2)\cdots(x-k+1)}{k!}, \quad x \in \mathbb{R}. \tag{3.7}$$

Όταν $x = n$ είναι ένας φυσικός αριθμός η τιμή του πολυωνύμου αυτού είναι $\binom{n}{k}$ και έχει τη συνδυαστική ερμηνεία που είδαμε παραπάνω. Όμως είναι χρήσιμο να ξέρουμε ότι η συνάρτηση αυτή του x ορίζεται μια χαρά και όταν το x είναι οποιοσδήποτε πραγματικός (ή μιγαδικός) αριθμός και μάλιστα η συνάρτηση αυτή είναι πολυώνυμο του x.

✏ **3.31**
Δείξτε ότι το πολυώνυμο $f(x) = \binom{x}{k}$ που ορίζεται στην (3.7) είναι ακεραιότιμο, *ισχύει δηλ. για κάθε ακέραιο $k \geq 0$*

$$x \in \mathbb{Z} \Longrightarrow f(x) \in \mathbb{Z}.$$

Βρείτε τις ρίζες αυτού του πολυωνύμου. Επίσης εκφράστε το διωνυμικό συντελεστή $\binom{-n}{k}$, όπου n θετικός ακέραιος, μέσω κάποιου άλλου διωνυμικού συντελεστή $\binom{N}{k}$, όπου N επίσης είναι θετικός ακέραιος.

✏ **3.32**
Ποια είναι τα διμελή υποσύνολα του $[4] = \{1, 2, 3, 4\}$.

Γράψτε μια συνάρτηση σε python που δοθέντος ενός συνόλου (ως μια λίστα python) να επιστρέφει μια λίστα με όλα τα διμελή υποσύνολα του συνόλου αυτού. Δουλέψτε συμπληρώνοντας την παρακάτω ημιτελή συνάρτηση.

```
def subsets2(s):
    n = len(s)
    ss = []
    if n <= 1:
        return ss
    else:
        for i in range(n):
        .......
        return ss
```

Η κλήση

```
s = ['a', 'b', 'c', 'd']
print subsets2(s)
```

θα πρέπει να σας επιστρέφει

```
[['a', 'b'], ['a', 'c'], ['a', 'd'], ['b', 'c'], ['b', 'd'], ['c', 'd']]
```

Παράδειγμα 3.4
Με πόσους τρόπους μπορούμε να διαλέξουμε τέσσερεις διαφορετικούς διψήφιους ακεραίους (δε μας ενδιαφέρει η σειρά τους) ούτως ώστε να χωρίζονται αυτοί σε δύο ζεύγη και οι αριθμοί κάθε ζεύγους να έχουν το ίδιο δεύτερο (χαμηλότερο) ψηφίο αλλά αριθμοί σε διαφορετικά ζεύγη να έχουν διαφορετικό δεύτερο ψηφίο;

Για να μετρήσουμε τους τρόπους σκεφτόμαστε με ποια διαδικασία θα παράγουμε μονοσήμαντα ένα τέτοιο αποτέλεσμα. Παρατηρούμε ότι στη δεύτερη θέση χρησιμοποιούνται ακριβώς δύο ψηφία, ένα στο ένα ζεύγος και ένα για το άλλο. Αποφασίζουμε λοιπόν κάθε τετράδα τέτοιων αριθμών να τη γράφουμε ως εξής:

$$xa, ya, zb, wb \tag{3.8}$$

όπου ισχύει

$$a, b \in \{0, \ldots, 9\},\ x, y, z, w \in \{1, \ldots, 9\},\ a > b,\ x > y,\ z > w. \tag{3.9}$$

Την τελευταία αυτή απαίτηση τη βάζουμε ώστε κάθε τετράδα από αυτές που θέλουμε να μετρήσουμε να γράφεται με μοναδικό *τρόπο στη μορφή (3.8). Πάντα δηλ. όταν είναι να γράψουμε μια τετράδα κάτω γράφουμε πρώτα το ζευγάρι όπου το ψηφίο των μονάδων είναι το μεγαλύτερο, και μέσα σε κάθε ζευγάρι γράφουμε πρώτα αυτόν τον αριθμό του οποίο το ψηφίο των δεκάδων είναι το μεγαλύτερο.*

Τα αντικείμενα δηλ. που θέλουμε να μετρήσουμε είναι σε ένα προς ένα αντιστοιχία με τις εξάδες

$$(a, b, x, y, z, w)$$

που ικανοποιούν την (3.9). Για να μετρήσουμε τις εξάδες αυτές μετράμε πρώτα πόσες είναι οι επιλογές μας για το ζεύγος a, b, πόσες για το ζεύγος x, y και πόσες για το ζεύγος z, w. Επειδή, λόγω της φύσης της συνθήκης (3.9), αυτές οι επιλογές είναι ανεξάρτητες μεταξύ τους μπορούμε να τις πολλαπλασιάσουμε. Αλλά για να επιλέξουμε το ζεύγος $a, b \in \{0, \ldots, 9\}$ με $a > b$ μπορούμε απλά να επιλέξουμε ένα διμελές υποσύνολο του $\{0, \ldots, 9\}$ και να ονομάσουμε a το μεγαλύτερο στοιχείο του και b το μικρότερο. Το πλήθος επιλογών μας δηλ. είναι $\binom{10}{2}$ και, ομοίως σκεπτόμενοι, βλέπουμε ότι για το ζεύγος x, y έχουμε $\binom{9}{2}$ επιλογές και ομοίως για το ζεύγος z, w.

Το τελικό αποτέλεσμα είναι λοιπόν

$$\binom{10}{2}\binom{9}{2}^2.$$

Παράδειγμα 3.5
Από μια συνηθισμένη τράπουλα με πόσους τρόπους μπορούμε να επιλέξουμε μια εξάδα από φύλλα υπό τον περιορισμό ότι ακριβώς τρία από αυτά είναι σπαθιά (♣); Οι εξάδες που επιλέγουμε είναι μη διατεταγμένες.

Για να απαντήσουμε βρίσκουμε μια διαδικασία παραγωγής του τυπικού αποτελέσματος. Αφού λοιπόν πρέπει τρία από αυτά τα χαρτιά να είναι σπαθιά ξεκινάμε διαλέγοντας πρώτα απ' όλα αυτά. Τα τρία αυτά φύλλα επιλέγονται χωρίς κανένα περιορισμό από τα 13 συνολικά σπαθιά της τράπουλας. Άρα οι δυνατότητες γι' αυτή την επιλογή είναι $\binom{13}{3}$.

Στη συνέχεια επιλέγουμε τα υπόλοιπα τρία φύλλα που πρέπει απλά να μην είναι σπαθιά, επιλέγονται δηλ. από τα $3 \times 13 = 39$ φύλλα που δεν είναι σπαθιά, δίνοντάς μας $\binom{39}{3}$ δυνατότητες.

Επειδή η πρώτη επιλογή (των σπαθιών) είναι ανεξάρτητη από τη δεύτερη το τελικό αποτέλεσμα είναι

$$\binom{13}{3} \cdot \binom{39}{3}.$$

Παράδειγμα 3.6
Είναι πολύ σημαντικό να τονίσουμε ότι η απαρίθμηση που κάναμε στο Παράδειγμα 3.5 είναι σωστή επειδή η μέθοδος κατασκευής έχει τις ακόλουθες ιδιότητες

- *Είναι τέτοια ώστε διαφορετικές επί μέρους επιλογές (στη μέθοδο κατασκευής που περιγράψαμε οι επί μέρους επιλογές ήταν δύο: πρώτα η επιλογή των σπαθιών και μετά η επιλογή των μη σπαθιών) οδηγούν αναγκαστικά σε διαφορετικό αποτέλεσμα, και*

- *Κάθε δυνατό αποτέλεσμα είναι δυνατό να κατασκευαστεί με τη μέθοδό μας.*

Οι δύο αυτές ιδιότητες μαζί εξασφαλίζουν ότι υπάρχει αμφιμονοσήμαντη αντιστοιχία ανάμεσα σε αυτά που κατασκευάζουμε και σε αυτά που θέλουμε να μετρήσουμε, άρα μπορούμε απλά να μετρήσουμε το πλήθος των αντικειμένων που κατασκευάζουμε.

Για να τονίσουμε το πόσο σημαντικές είναι αυτές οι δύο ιδιότητες και πόσο προσεκτικοί πρέπει να είμαστε σε αντίστοιχα μετρήματα, ας παραλλάξουμε λίγο το ερώτημα του Παραδείγματος 3.5. Ας ρωτήσουμε το ίδιο με μόνη διαφορά ότι τώρα δεν απαιτούμε ακριβώς *τρία φύλλα να είναι σπαθιά αλλά* τουλάχιστον *τρία.*

Ας βρούμε μια διαδικασία κατασκευής (σύνθετη επιλογή). Αφού όπωσδήποτε θέλουμε τρία σπαθιά ας ξεκινήσουμε επιλέγοντάς τα. Έχουμε πάλι $\binom{13}{3}$ δυνατότητες γι' αυτή την επιλογή. Στο δεύτερο στάδιο μένει απλά να επιλέξουμε άλλα τρία φύλλα από τα εναπομέναντα 49, αφού τώρα δε μας πειράζει να έχουμε επιπλέον σπαθιά. Στο δεύτερο στάδιο λοιπόν έχουμε $\binom{49}{3}$ δυνατότητες. Εφ' όσον τα δύο στάδια επιλογής είναι ημι-ανεξάρτητα (προηγουμένως ήταν ανεξάρτητα) μπορούμε και πάλι να πολλαπλασιάσουμε και παίρνουμε τελικό αποτέλεσμα

$$\binom{13}{3}\cdot\binom{49}{3}.$$

ΛΑΘΟΣ!

Και ο λόγος είναι ότι μπορούμε να έχουμε το ίδιο αποτέλεσμα ακόμη κι αν η σύνθετη επιλογή μας αλλάξει. Για παράδειγμα, η κατασκευή μας μπορεί στο πρώτο στάδιο να μας δώσει 1 ♣, 2 ♣, 3 ♣ και στο δεύτερο 4 ♣, 1 ♡ και 2 ♡. Μπορεί επίσης να μας δώσει στο πρώτο στάδιο 1 ♣, 2 ♣, 4 ♣ και στο δεύτερο να μας δώσει 3 ♣, 1 ♡ και 2 ♡. Η τελική εξάδα είναι στις δύο αυτές περιπτώσεις η ίδια. Άρα ο αριθμός $\binom{13}{3}\cdot\binom{49}{3}$ που υπολογίσαμε προηγουμένως είναι αυστηρά (και μάλλον κατά πολύ) μεγαλύτερος της πραγματικότητας.

Πώς μπορούμε να διορθώσουμε τη μέθοδό μας; Μια απλή απάντηση είναι ότι μπορούμε να διαχωρίσουμε τις δυνατές εξάδες σε τέσσερεις κατηγορίες: αυτές που έχουν ακριβώς 3, ακριβώς 4, ακριβώς 5 ή ακριβώς 6 σπαθιά. Μπορούμε εύκολα να μετρήσουμε τις εξάδες κάθε κατηγορίας, ουσιαστικά με τη μέθοδο του Παραδείγματος 3.5, και στο τέλος να προσθέσουμε αυτά τα τέσσερα νούμερα. Έτσι το αποτέλεσμα είναι

$$\binom{13}{3}\binom{39}{3}+\binom{13}{4}\binom{39}{2}+\binom{13}{5}39+\binom{13}{6}$$

όπου ο κάθε προσθετέος αντιπροσωπεύει και μια κατηγορία. (Βεβαιωθείτε ότι καταλαβαίνετε αυτή την αντιστοιχία.)

Παράδειγμα 3.7

Αν αναπτύξουμε (γράψουμε δηλ. στη μορφή $a_0+a_1x+a_2x^2+\cdots+a_nx^n$) το πολυώνυμο $(1+x)^{10}$ ποιος είναι ο συντελεστής του x^4;

Ας σκεφτούμε λίγο πώς υπολογίζει κανείς το ανάπτυγμα ενός γινομένου, για απλότητα του $(a+b)^2=(a+b)(a+b)$ που έχει δύο μόνο παράγοντες και όχι 10 όπως αυτό που ζητάμε. Το βρίσκουμε παίρνοντας κάθε προσθετέο του πρώτου αθροίσματος πολλαπλασιασμένο με κάθε προσθετέο του δεύτερου, και αθροίζουμε τα αποτελέσματα. Αν λοιπόν ρωτήσουμε ποιός είναι ο συντελεστής του ab στο ανάπτυγμα, είναι σα να ρωτάμε με πόσους τρόπους μπορεί να εμφανιστεί το γινόμενο ab κάνοντας το ανάπτυγμα όπως παραπάνω.

Λόγω αντιμεταθετικότητας του πολλαπλασιασμού αυτό μπορεί να εμφανιστεί είτε ως ab είτε ως ba. Το ab εμφανίζεται ακριβώς μία φορά, όταν συνδυάζουμε στο ανάπτυγμα το a από την πρώτη παρένθεση με το b από τη δεύτερη. Δεν υπάρχει άλλος τρόπος. Ομοίως μία φορά εμφανίζεται και το ba όταν συνδυάζεται το b από την πρώτη παρένθεση με το a από τη δεύτερη. Άρα ο συντελεστής του ab στο ανάπτυγμα είναι $1+1=2$. Ομοίως τα a^2 και b^2 μπορούν το καθένα να προκύψουν με ένα μόνο τρόπο. Για το a^2, π.χ., πρέπει να επιλεγεί το a και από την πρώτη και από τη δεύτερη παρένθεση, ομοίως και για το b^2. Επιβεβαιώνεται έτσι ο γνωστός μας τύπος $(a+b)^2=a^2+2ab+b^2$.

Αν ρωτήσουμε για το συντελεστή του a^2b στο ανάπτυγμα του $(a+b)^3$ είναι σα να ρωτάμε με πόσους τρόπους μπορούμε να συνδυάσουμε ένα b με δύο a από τις τρείς παρενθέσεις $(a+b)$ που υπάρχουν στο

γινόμενο. Αυτό μπορεί να γίνει με ακριβώς τρείς τρόπους μια και αρκεί να πούμε από ποια παρένθεση επιλέγουμε να πάρουμε το b. Αυτό προσδιορίζει ότι από τις άλλες δύο παίρνουμε από ένα a.

Επανερχόμαστε τώρα στο αρχικό μας ερώτημα και ρωτάμε για το συντελεστή του x^4 στο ανάπτυγμα του $(1+x)^{10}$. Στο ανάπτυγμα αυτό οι προσθετέοι προκύπτουν με επιλογή, ο καθένας, ενός 1 ή ενός x από κάθε μία από τις 10 παρενθέσεις. Το x^4 λοιπόν μπορεί να προκύψει με τόσους τρόπους όσοι είναι οι τρόποι να επιλέξουμε τις 4 παρενθέσεις, από τις οποίες θα πάρουμε τα x. Άρα το αποτέλεσμα είναι

$$\binom{10}{4}.$$

✏ **3.33**
Από μια ομάδα 10 ατόμων, με πόσους τρόπους μπορεί να επιλεγεί ένα τριμελές προεδρείο χωρίς διακριτούς ρόλους; Ένα 5μελές προεδρείο με πρόεδρο, αντιπρόεδρο και 3 μέλη;


Για το δεύτερο ερώτημα, επιλέξτε το προεδρείο επιλέγοντας πρώτα τον πρόεδρο, μετά τον αντιπρόεδρο και, τέλος, τα τρία μέλη μαζί.

✏ **3.34**
Μέ πόσους τρόπους μπορούμε να επιλέξουμε, από μια συνηθισμένη τράπουλα με 52 φύλλα (που χωρίζονται σε 4 χρώματα και 13 είδη), πέντε φύλλα από τα οποία 2 κόκκινα ($\diamondsuit$ ή $\heartsuit$) και 3 σπαθιά; Δε μας ενδιαφέρει η σειρά επιλογής των φύλλων.

✏ **3.35**
Αν n άρτιο για ποιο $k \in \{0,1,\ldots,n\}$ μεγιστοποιείται η ποσότητα $\binom{n}{k}$; Τι γίνεται αν n περιττός;

✏ **3.36**
Δείξτε την ταυτότητα

$$\sum_{k=0}^{n}\binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n,$$

για κάθε $n \geq 0$.

✏ **3.37**
Δείξτε την ταυτότητα

$$\binom{n}{k} = \binom{n}{n-k}$$

για κάθε $n \geq 0$ και $0 \leq k \leq n$.

✏ **3.38**
Αν r, s, k είναι φυσικοί αριθμοί με $r \geq s$ δείξτε ότι ο αριθμός $s!$ είναι διαιρέτης του

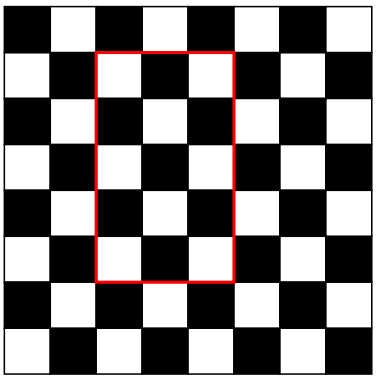
$$(k+1)(k+2)\cdots(k+r).$$

3.3 Επαναληπτικές ασκήσεις Κεφαλαίου

✏ **3.39**
Πόσα διμελή υποσύνολα του $[50] = \{1,2,\ldots,50\}$ υπάρχουν όπου ο ένας αριθμός του ζεύγους είναι διπλάσιος από τον άλλο;

✏ **3.40**
Σε μια 8×8 σκακιέρα πόσα διαφορετικά ορθογώνια ορίζονται; Ένα ορθογώνιο είναι ένα υποσύνολο των κελιών (τετραγώνων) της σκακιέρας που έχει σχήμα ορθογωνίου. Δύο ορθογώνια θεωρούνται διαφορετικά αν είναι διαφορετικά ως σύνολα κελιών.

Δείτε στο Σχήμα 3.5.



Σχήμα 3.5: Μια 8×8 σκακιέρα κι ένα από τα ορθογώνια τα οποία θέλουμε να μετρήσουμε

✏ **3.41**
Με πόσους τρόπους μπορούμε να διατάξουμε τα ψηφία $1, 2, \ldots, 9$ *ώστε ανάμεσα στο 1 και το 2 να υπάρχουν ακριβώς τρία ψηφία;*

✏ **3.42**
Με πόσους τρόπους μπορούμε να διατάξουμε τα ψηφία $1, 2, \ldots, 9$ *ώστε το 1 να προηγείται του 2 και το 2 να προηγείται του 3;*

✏ **3.43**
Πόσες μεταθέσεις των αριθμών $1, 2, 3, \ldots, 2n-1, 2n$ *υπάρχουν που στις άρτιες θέσεις έχουν μόνο άρτιους αριθμούς;*

Πόσες υπάρχουν που σε τουλάχιστον μια άρτια θέση υπάρχει άρτιος αριθμός;

✏ **3.44**
Πόσα υποσύνολα του $\{1, 2, \ldots, 2n\}$ *περιέχουν ακριβώς* k *περιττούς αριθμούς;*

✏ **3.45**
Σε μια σχολή χορού μια τάξη αποτελείται από 12 άνδρες και 10 γυναίκες. Με πόσους τρόπους μπορούν να επιλεγούν 5 άνδρες και 5 γυναίκες και να σχηματίσουν ζεύγη χορού; Δε μας ενδιαφέρει η σειρά των ζευγών, μόνο το ποια ζεύγη σχηματίζονται.

✏ **3.46**
Με πόσους τρόπους μπορούμε να επιλέξουμε ένα άνδρα και μια γυναίκα, που να μην είναι μεταξύ τους παντρεμένοι, από n *παντρεμένα ζευγάρια;*

✏ **3.47**
Με πόσους τρόπους μπορούμε να χωρίσουμε τους αριθμούς $\{1, 2, 3, \ldots, 2n\}$ *σε* n *ζεύγη όταν (α) μας ενδιαφέρει η σειρά των ζευγών και (β) όταν δε μας ενδιαφέρει;*

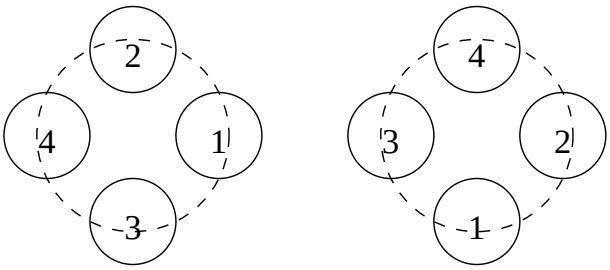
✏ **3.48**
Στην Άσκηση 3.19 υποθέστε ότι κάθε άνδρας παντρεύεται όσες γυναίκες θέλει αλλά μια γυναίκα δε μπορεί να παντρευτεί ταυτόχρονα παραπάνω από έναν άνδρα. Με πόσους τρόπους μπορείτε να παντρέψετε και τους 5 άνδρες ώστε και οι 7 γυναίκες να παντρευτούν.

✏ **3.49**
Με πόσους τρόπους μπορούν να υπάρξουν n *ζευγαρώματα ανάμεσα σε* n *άνδρες και* n *γυναίκες;*

✏ **3.50**
Πόσους διαιρέτες έχει ο αριθμός 2^m*; Ο αριθμός* $2^m 3^n$*;*

✏ **3.51**

Πόσες κυκλικές μεταθέσεις *του συνόλου* $[n]$ *υπάρχουν; Μια κυκλική μετάθεση του* $[n]$ *είναι ένας τρόπος να γράψουμε τα στοιχεία του σε κύκλο (ώστε κάθε στοιχείο να έχει ένα προηγούμενο και ένα επόμενο), αλλά δύο κυκλικές μεταθέσεις που μπορούν να ταυτιστούν με μια στροφή του κύκλου θεωρούνται ίδιες. Για παράδειγμα, για* $n = 4$*, οι μεταθέσεις* (1243) *και* (3124) *θεωρούνται ίδιες. (Δείτε το Σχήμα 3.6.)*



Σχήμα 3.6: Οι δύο κυκλικές τοποθετήσεις των αριθμών 1,2,3,4 μπορούν να ταυτιστούν με μια στροφή 90 μοιρών, άρα θεωρούνται ίδιες κυκλικές μεταθέσεις

✏ **3.52**

Αν n *είναι περιττός αριθμός δείξτε ότι*

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots + \binom{n}{n-1} = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots + \binom{n}{n}.$$

Ερμηνεύστε και τις δυο μεριές της ισότητας ως το πλήθος κάποιων υποσυνόλων του $[n]$*. Δείξτε έπειτα ότι οι δυο αυτές οικογένειες υποσυνόλων του* $[n]$ *(των οποίων τα μεγέθη είναι το αριστερό και το δεξί μέλος της ισότητας) είναι ισοπληθικές δείχνοντας μια μεταξύ τους 1-1 και επί αντιστοίχιση.*

✏ **3.53**

Από μια συνηθισμένη τράπουλα με πόσους τρόπους μπορούμε να επιλέξουμε 6 χαρτιά (δε μας ενδιαφέρει η σειρά τους) από τα οποία τα τρία να είναι κόκκινα (♢ ή ♡) και τα τρία μαύρα (♠ ή ♣), και τα δύο από τα τρία κόκκινα να είναι ίδιου είδους (αριθμού).

Μια τέτοια δυνατή εξάδα είναι η:

$$1♢, 1♡, 2♡, 1♠, 2♠, 3♣$$

✏ **3.54**

Πόσες διαφορετικές λέξεις με 10 γράμματα υπάρχουν που να έχουν μέσα τρία γράμματα Α, τέσσερα Β και στις υπόλοιπες θέσεις οποιαδήποτε άλλα γράμματα (από τα 24 κεφαλαία της ελληνικής γλώσσας);

Δε μας ενδιαφέρει να είναι λέξεις με κάποιο νόημα. Λέξη μήκους n *είναι μια σειρά από* n *γράμματα από αυτά που επιτρέπουμε και τίποτα παραπάνω.*

✏ **3.55**

Σ' ένα μικροβιολογικό εργαστήριο έχουν 100 φιάλες αίματος από διαφορετικά άτομα και γνωρίζουν ότι ακριβώς μια από αυτές περιέχει αίμα μολυσμένο με μια ουσία Α. Ο έλεγχος για το αν ένα δείγμα αίματος περιέχει την ουσία Α είναι πολύ ακριβός και το εργαστήριο θέλει να ελαχιστοποιήσει τον αριθμό δειγμάτων που θα ελέγξει για να βρει τη μολυσμένη φιάλη.

Γι' αυτό το λόγο το εργαστήριο δημιουργεί N *μίγματα από τα 100 μπουκάλια που θέλει να ελέγξει και στέλνει αυτά τα* N *δείγματα σε ένα εργαστήριο στην Αμερική το οποίο στέλνει πίσω τις απαντήσεις. (Τα ταχυδρομικά είναι επίσης πανάκριβα, οπότε το εργαστήριο στέλνει και τα* N *μίγματα με μια αποστολή.)*

Αν κάποιο από αυτά τα μίγματα προκύψει θετικό αυτό σημαίνει ότι κάποιο από τα μπουκάλια που χρησιμοποιήθηκαν στο μίγμα αυτό είναι μολυσμένο.

Ποιος είναι ο ελάχιστος αριθμός μιγμάτων N που πρέπει να στείλει το εργαστήριο για να βρει τη μολυσμένη φιάλη, και με ποια μίγματα;

✏ **3.56**
Έχουμε n αριθμημένες μπάλες ($n > 2$) και κάμποσα, επίσης αριθμημένα, χρωματιστά κουτιά, κάποια από τα οποία είναι βαμμένα κόκκινα, κάποια μπλε και κάποια είναι άβαφα (υπάρχουν και από τα τρία είδη κουτιών).

Ας είναι A το πλήθος των τρόπων με τους οποίους μπορούν αυτές οι μπάλες να τοποθετηθούν αποκλειστικά στα άβαφα κουτιά και B το πλήθος των τρόπων με τους οποίους μπορούν αυτές οι μπάλες να τοποθετηθούν σε κουτιά που είναι όλα του ίδιου χρώματος (κόκκινου ή μπλε).

Δείξτε ότι πάντα $A \neq B$.

✏ **3.57**
Μια ομάδα 7 ληστών μόλις διέπραξε μια πολύ επιτυχημένη ληστεία τράπεζας. Τα χρήματα που σήκωσαν τα έχουν βάλει σε ένα χρηματοκιβώτιο στο καταφύγιό τους. Πρέπει όμως να διαφυλάξουν αυτά τα χρήματα πρώτ' απ' όλα από τους ίδιους τους τους εαυτούς.

Τι θα γίνει π.χ. αν σηκωθεί ένας από αυτούς τα πάρει και φύγει; Αυτό φυσικά δεν είναι αποδεκτό στην ομάδα. Ή αν δύο από αυτούς συμφωνήσουν μεταξύ τους και τα πάρουν και φύγουν; Ούτε κι αυτό είναι αποδεκτό.

Όμως πρόκειται για μια ομάδα κλεφτών μεγαλωμένη από τους γονείς τους με πίστη στα δημοκρατικά ιδεώδη. Αν λοιπόν κάποιοι 4 από αυτούς αποφασίσουν να τα πάρουν αυτό γίνεται αποδεκτό γιατί οι 4 είναι πλειοψηφία στους 7. Όχι όμως 3 ή λιγότεροι.

Πώς θα το υλοποιήσουν αυτό; Το χρηματοκιβώτιο έχει απ' έξω ένα μεγάλο σίδερο πάνω στο οποίο μπορούν να μπουν πολλά λουκέτα και όλα αυτά πρέπει να ξεκλειδωθούν για να ανοίξει. Για κάθε λουκέτο μπορούμε να έχουμε όσα αντικλείδια χρειαζόμαστε.

Πρέπει λοιπόν να δώσουμε σε κάθε κλέφτη ένα σετ από κλειδιά με τέτοιο τρόπο ώστε:

1. *Οποιοιδήποτε 4 κλέφτες να έχουν μεταξύ τους όλα τα κλειδιά που απαιτούνται για να ανοίξει το χρηματοκιβώτιο.*
2. *Για οποιουσδήποτε 3 κλέφτες αυτό δε συμβαίνει.*

Πώς μπορεί να γίνει αυτό; Πόσα λουκέτα συνολικά χρειάζονται και ποια κλειδιά θα πάρει κάθε κλέφτης;

3.4 Video Κεφαλαίου

3.1
Αρχή Πολλαπλασιασμού Ανεξάρτητων Επιλογών (video και συνοδευτικές ασκήσεις, 6:12 λεπτά).

3.2
Αρχή Πολλαπλασιασμού Ανεξάρτητων Επιλογών. Παραδείγματα. (video και συνοδευτικές ασκήσεις, 16:29 λεπτά).

3.3
Αρχή Πολλαπλασιασμού Ημιανεξάρτητων Επιλογών. Παραδείγματα. Μεταθέσεις. (video και συνοδευτικές ασκήσεις, 11:00 λεπτά).

3.4
Συνδυασμοί n αντικειμένων ανά k. Διωνυμικοί συντελεστές. (video και συνοδευτικές ασκήσεις, 15:51 λεπτά).

3.5
Παράδειγμα: Πόσες εξάδες με τρία σπαθιά; (video και συνοδευτικές ασκήσεις, 14:07 λεπτά).

Βιβλιογραφία Κεφαλαίου

[1] Peter J Cameron. *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, 1994.

[2] Ronald L Graham, Donald E Knuth, and Oren Patashnik. *Concrete Mathematics*. 1994.

[3] Chung Laung Liu and CL Liu. *Elements of discrete mathematics*. McGraw-Hill New York, 1985.

[4] Richard P Stanley. *Enumerative combinatorics*. 1986.

Κεφάλαιο 4

Προχωρημένη απαρίθμηση

Κύριες βιβλιογραφικές αναφορές για αυτό το Κεφάλαιο είναι οι C. L. Liu and C. Liu 1985, Graham, Knuth, and Patashnik 1994, Cameron 1994 και Stanley 1986.

4.1 Διαμερίσεις και συνδυασμοί με επανάθεση

Ας συμβολίσουμε με $P(n,r)$ το πλήθος των τρόπων με τους οποίους μπορούμε να γράψουμε τον φυσικό αριθμό n ως άθροισμα r μη αρνητικών ακεραίων $x_1,\ldots,x_r$:

$$n = x_1 + \cdots + x_r.$$

Για παράδειγμα, αν $n=3$ και $r=2$ οι τρόποι αυτοί είναι οι

$$3 = 3+0 = 2+1 = 1+2 = 0+3 \tag{4.1}$$

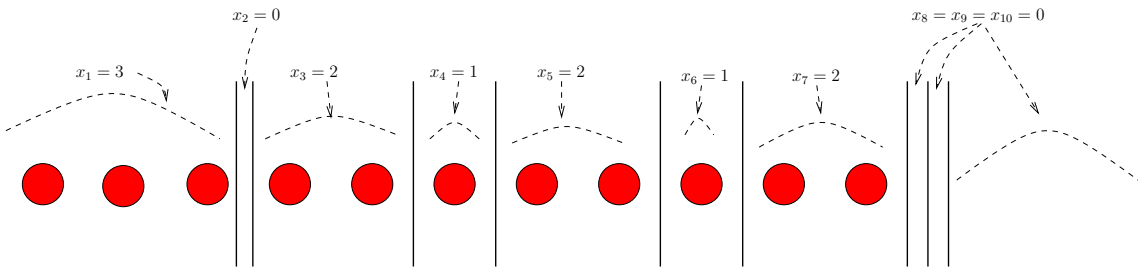
και άρα $P(3,2) = 4$. Η σειρά των προσθετέων $x_1,\ldots,x_r$ έχει σημασία. Την ποσότητα $P(n,r)$ την ονομάζουμε *πλήθος διαμερίσεων του n σε r κομμάτια*. Παρατηρήστε ότι δεν απαιτούμε το r να είναι $\leq n$ αφού το μέγεθος των κομματιών μπορεί να είναι και 0.

Θεώρημα 4.1
Αν $n \geq 0$ και $r \geq 0$ τότε ισχύει

$$P(n,r) = \binom{n+r-1}{n} = \binom{n+r-1}{r-1}. \tag{4.2}$$

Απόδειξη

Παριστάνουμε τον αριθμό n σα n μπάλες στη σειρά και την τυχούσα διαμέριση του n, δηλ. τον τυχόντα τρόπο να γράψουμε $n = x_1+\cdots+x_r$, σαν ένα χωρισμό αυτής της σειράς από μπάλες με $r-1$ τοιχώματα (δείτε Σχήμα 4.1).



Σχήμα 4.1: Χωρίζοντας $n = 11$ μπάλες σε $r = 10$ ομάδες με 9 ενδιάμεσα τοιχώματα

Η τιμή του x_1 βρίσκεται αν μετρήσουμε πόσες μπάλες υπάρχουν από το $-\infty$ έως το πρώτο τοίχωμα, το x_2 αν μετρήσουμε τις μπάλες από το πρώτο έως το δεύτερο τοίχωμα, κλπ. Τέλος το x_r βρίσκεται αν μετρήσουμε τις μπάλες από το τελευταίο (υπ' αριθμόν $r-1$) τοίχωμα έως το $+\infty$.

Άρα, για να μετρήσουμε το πλήθος των διαμερίσεων $P(n,r)$ αρκεί να μετρήσουμε πόσα διαφορετικά σχήματα σαν και αυτό του Σχήματος 4.1 υπάρχουν, αφού είναι φανερό ότι σε κάθε τέτοιο σχήμα αντιστοιχεί και μια διαφορετική διαμέριση, και αντίστροφα.

Με ποια διαδικασία μπορούμε λοιπόν να κατασκευάσουμε μονοσήμαντα ένα τέτοιο σχήμα; Το κάνουμε ως εξής: βάζουμε πρώτα στη σειρά $n+r-1$ αντικείμενα και κατόπιν ονομάζουμε τα n από αυτά μπάλες και τα υπόλοιπα $r-1$ τοιχώματα. Αυτό μπορεί να γίνει ακριβώς με $\binom{n+r-1}{n}$ τρόπους. Η δεύτερη ισότητα μέσα στο συμπέρασμα του Θεωρήματος 4.1 είναι απλή συνέπεια της ταυτότητας $\binom{a}{b} = \binom{a}{a-b}$ (δείτε την Άσκηση 3.37).

■

Για παράδειγμα σύμφωνα με το Θεώρημα 4.1 ισχύει $P(3,2) = \binom{3+2-1}{3} = \binom{4}{3} = 4$ το οποίο συμφωνεί με την (4.1).

✏ **4.1**
Βρείτε όλες τις διαμερίσεις του 4 σε 3 κομμάτια.

Πέρα από τη σημασία που έχει το ίδιο το πρόβλημα του να μετρήσουμε το πλήθος των διαμερίσεων του n σε r κομμάτια, το ερώτημα αποκτά μεγαλύτερη σημασία γιατί είναι ένας ισοδύναμος τρόπος του να ρωτήσουμε το εξής:

> Με πόσους τρόπους μπορούμε να επιλέξουμε k από n στοιχεία όταν κάθε στοιχείο από τα n μπορεί να επιλεγεί ένα απεριόριστο αριθμό από φορές, και όταν δε μας ενδιαφέρει η σειρά των επιλεγέντων στοιχείων;

Ένας ισοδύναμος τρόπος να θέσουμε το ίδιο ερώτημα είναι ο ακόλουθος. Έχουμε ένα σάκο που έχει μέσα n μπάλες. Οι μπάλες φέρουν η κάθε μια τον αριθμό της. Επαναλαμβάνουμε k φορές την πράξη:

> Παίρνουμε μια μπάλα από το σάκο και γράφουμε σ' ένα χαρτί τον αριθμό της. Έπειτα επανατοποθετούμε τη μπάλα στο σάκο.

Στο τέλος παρατηρούμε τους k αριθμούς που γράψαμε, χωρίς να μας ενδιαφέρει η σειρά τους. Πόσα είναι τα δυνατά διαφορετικά αποτελέσματα; Από αυτή την εναλλακτική περιγραφή προκύπτει και το όνομα *συνδυασμοί n στοιχείων ανά k με επανάθεση*. Το πλήθος αυτών των συνδυασμών συμβολίζεται με $\left\langle {n \atop k} \right\rangle$.

Παράδειγμα 4.1
Οι συνδυασμοί του συνόλου $\{A,B\}$ ανά 3 με επανάθεση είναι οι

$$AAA, AAB, ABB, BBB.$$

Για παράδειγμα, ο συνδυασμός ABB θεωρείται ίδιος με τον BAB μια και τα στοιχεία διαφέρουν μόνο στη σειρά εμφάνισης.

✏ **4.2**
Δείξτε ότι για κάθε n ισχύει $\left\langle {n \atop 1} \right\rangle = n$. Επίσης ότι, για $n \geq 2$, ισχύει $\left\langle {n \atop 2} \right\rangle = n + \binom{n}{2}$.

✏ **4.3**
Βρείτε το X στην ισότητα

$$\left\langle {n \atop 3} \right\rangle = \binom{n}{3} + X.$$

Σκεφθείτε συνδυαστικά. Μη χρησιμοποιήσετε τον τύπο που δείχνουμε παρακάτω στο Θεώρημα 4.2 παρά μόνο για να ελέγξετε το αποτέλεσμά σας.

Ομοίως σκεπτόμενοι βρείτε τη διαφορά $\left\langle {n \atop 4} \right\rangle - \binom{n}{4}$.

Στο τέλος αυτής της διαδικασίας επιλογής k στοιχείων με επανάθεση έχουμε στα χέρια μας k αριθμούς, όχι κατ' ανάγκη διαφορετικούς μεταξύ τους, κάθε ένας από τους οποίους ανήκει στο σύνολο $\{1, \ldots, n\}$. Έστω x_i, $i = 1, \ldots, n$, το πλήθος αυτών των αριθμών που είναι ίσοι με i. Επειδή δε μας ενδιαφέρει η σειρά που εμφανίζεται κάθε ένα από τα νούμερα που επιλέγουμε, αλλά μόνο το πόσες φορές εμφανίζεται, γίνεται φανερό ότι

$$x_1 + \cdots + x_n = k \tag{4.3}$$

και ότι κάθε διαφορετικό αποτέλεσμα της επιλογής με επανάθεση αντιστοιχεί και σε μια διαφορετική n-άδα $x_1, \ldots, x_n$ που ικανοποιεί την (4.3). Έχουμε έτσι αποδείξει το ακόλουθο.

Θεώρημα 4.2
Τα δυνατά αποτελέσματα επιλογής k αντικειμένων από n με επανάθεση είναι ίσα σε πλήθος με τις δυνατές διαμερίσεις του k σε n κομμάτια. Έχουμε δηλαδή

$$\left\langle {n \atop k} \right\rangle = \binom{n+k-1}{k}.$$

✏ **4.4**
Αν επιλέξουμε k αντικείμενα από n με επανάθεση και δεν αγνοήσουμε τη σειρά των επιλογών (π.χ., αν επιλέγουμε 3 αντικείμενα από τα Α, Β με επανάθεση, τα αποτελέσματα ΑΑΒ και ΑΒΑ θεωρούνται τώρα διαφορετικά), πόσες διαφορετικές επιλογές υπάρχουν;

✏ **4.5**
Αν έχετε ένα σωρό από άπειρες όμοιες μπάλες και n αριθμημένα κουτιά χωρητικότητας n μπαλών το καθένα με πόσους τρόπους μπορείτε να τοποθετήσετε κάποιες μπάλες στα κουτιά;

Ίδιο ερώτημα αν τα κουτιά δεν είναι αριθμημένα.

✏ **4.6**
Σε ένα ασανσέρ μπαίνουν 8 άτομα στο ισόγειο ενός κτηρίου. Ξεκινάει την πορεία του προς τα πάνω από το ισόγειο (όροφος 0) και σταματάει στον τελευταίο όροφο που είναι ο όροφος Νο 6.

Με πόσους διαφορετικούς τρόπους μπορεί να έχουν συμβεί οι αποβιβάσεις των 8 ατόμων αν

1. *Οι 8 επιβάτες είναι πανομοιότυποι μεταξύ τους.*

2. *Υπάρχουν 5 άνδρες επιβάτες και 3 γυναίκες. Άτομα του ίδιου φύλου δεν ξεχωρίζουν μεταξύ τους.*

3. *Κάντε τις προηγούμενες περιπτώσεις υποθέτοντας ότι συμβαίνει τουλάχιστον μια αποβίβαση στον 6ο όροφο (αλλιώς δε θα είχε λόγο το ασανσέρ να ανέβει ως εκεί) ή, αντίθετα, χωρίς να υποθέσετε κάτι τέτοιο (υποθέστε δηλ. ότι το ασανσέρ πάντα πάει ως τον 6ο, ακόμη κι αν δεν έχει να αποβιβάσει κάποιον εκεί).*

✏ **4.7**
Με πόσους τρόπους μπορούμε να επιλέξουμε τους ακεραίους $x_1, x_2, \ldots, x_k$ τ.ώ. να ισχύει $1 \leq x_1 < x_2 < \cdots < x_k \leq n$;

✏ **4.8**
Αποδείξτε ότι, για k σταθερό, η συνάρτηση

$$\left\langle {n \atop k} \right\rangle - \binom{n}{k}$$

είναι πολυώνυμο του n και ότι, ανάλογα με το αν το k είναι άρτιο ή περιττό, το πολυώνυμο αυτό περιέχει ή μόνο άρτιες δυνάμεις του n ή μόνο περιττές. Βρείτε το άθροισμα των συντελεστών του πολυωνύμου αυτού.

Παράδειγμα 4.2
(Αλυσίδες DNA κατά Gamow) *Μια αλυσίδα DNA είναι μια πεπερασμένη σειρά από χημικές βάσεις. Οι βάσεις αυτές είναι γνωστές με τα σύμβολα A, C, G και T. Ένα αμινοξύ είναι μια αλυσίδα DNA και είναι γνωστό ότι υπάρχουν ακριβώς 20 αμινοξέα. Αν υποθέσουμε ότι όλα τα αμινοξέα είναι αλυσίδες με το ίδιο μήκος, τότε εύκολα βλέπουμε ότι το μήκος αυτό δε μπορεί να είναι 1 ή 2. Πράγματι υπάρχουν ακριβώς 4 αλυσίδες μήκους 1 (οι A, C, G και T) και $4^2 = 16$ αλυσίδες μήκους 2 (αυτό γιατί μια τέτοια αλυσίδα ορίζεται από δύο επιλογές με 4 δυνατότητες για την κάθε μία). Από την άλλη μεριά οι αλυσίδες DNA μήκους 3 είναι το πλήθος $4^3 = 64$, είναι δηλ. περισσότερες από 20.*

Το 1954 ο G. Gamow πρότεινε ότι δύο αλυσίδες DNA κωδικοποιούν το ίδιο αμινοξύ αν και μόνο αν περιέχουν τις ίδιες βάσεις ανεξαρτήτως σειράς. Οι αλυσίδες δηλ. ACC και CAC, αν και διαφορετικές, κωδικοποιούν το ίδιο αμινοξύ. Αν η υπόθεση του Gamow είναι σωστή πόσα διαφορετικά αμινοξέα κωδικοποιούνται με αλυσίδες DNA μήκους 3; Με λίγη σκέψη βλέπουμε ότι το πλήθος των διαφορετικών αμινοξέων είναι το ίδιο με το πλήθος των διαφορετικών συνδυασμών των τεσσάρων γραμμάτων A, C, G και T ανά τρία, με επανάθεση. Ο αριθμός αυτός είναι δηλ.

$$\left\langle \begin{matrix} 4 \\ 3 \end{matrix} \right\rangle = \binom{4+3-1}{3} = \binom{6}{3} = \frac{6 \cdot 5 \cdot 4}{3!} = 20,$$

συμφωνεί δηλ. η υπόθεση του Gamow με το πειραματικά διαπιστωμένο γεγονός ότι υπάρχουν ακριβώς 20 αμινοξέα. Όμως, για άλλους λόγους, η υπόθεση του Gamow έχει αποδειχθεί ότι δεν ισχύει.

✏ **4.9**
Με πόσους τρόπους μπορούμε να τοποθετήσουμε n όμοιες μπάλες σε k κουτιά που είναι αριθμημένα με τους αριθμούς 1 έως k;

Ίδιο ερώτημα όταν και οι μπάλες είναι αριθμημένες.

Παράδειγμα 4.3
(Η κατανομή Bose-Einstein στη στατιστική μηχανική)
Στη στατιστική μηχανική εξετάζουμε ένα σύστημα από t σωμάτια κάθε ένα από τα οποία μπορεί να βρίσκεται σε p διαφορετικές καταστάσεις, π.χ. σε p διαφορετικά ενεργειακά επίπεδα. Μια κατάσταση *του συστήματος είναι η περιγραφή της κατάστασης του κάθε σωματιδίου. Όταν τα σωμάτια είναι ίδια μεταξύ τους υποθέτουμε συνήθως ότι δεν έχει σημασία ποια από τα t σωμάτια είναι στο κάθε ενεργειακό επίπεδο αλλά μόνο πόσα. Η υπόθεση ότι όλες αυτές οι καταστάσεις είναι εξίσου πιθανές λέγεται κατανομή Bose-Einstein.*

Στο μοντέλο Bose-Einstein πόσες διαφορετικές καταστάσεις του συστήματος υπάρχουν; Αν θέσουμε x_i, $i = 1, \ldots, p$, να είναι το πλήθος των σωματίων στο ενεργειακό επίπεδο i, τότε πρέπει απλά να διαλέξουμε τους μη αρνητικούς ακεραίους x_i ώστε να έχουν άθροισμα t. Δηλαδή το πλήθος καταστάσεων του συστήματος είναι ίσο με το πλήθος των διαμερίσεων του t σε p κομμάτια, δηλ.

$$\binom{t+p-1}{t}.$$

✏ **4.10**
Στην κατανομή Fermi-Dirac υποθέτουμε ότι τα t σωμάτια είναι όλα όμοια και ότι δε μπορούν δύο σωμάτια να βρίσκονται στο ίδιο ενεργειακό επίπεδο (υπάρχουν p ενεργειακά επίπεδα). Αν $t \leq p$ πόσες διαφορετικές καταστάσεις του συστήματος σωματίων υπάρχουν; (Δείτε το Παράδειγμα 4.3 και την Άσκηση 4.9.)

4.2 Πολυωνυμικοί συντελεστές

Έχουμε δεί ότι αν θέλουμε να επιλέξουμε k αντικείμενα από n, χωρίς επανάθεση, το πλήθος των τρόπων να γίνει αυτό είναι

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Τι γίνεται αν θέλουμε να επιλέξουμε, πάλι χωρίς επανάθεση, μια ομάδα στοιχείων του $\{1,\ldots,n\}$ μεγέθους k_1, μια ομάδα μεγέθους k_2, κλπ, και τέλος μια ομάδα μεγέθους k_r, όπου για $j=1,\ldots,r$ έχουμε $0\le k_j\le n$ και επιπλέον ισχύει $k_1+\cdots+k_r=n$; Με πόσους τρόπους δηλ. μπορούμε να διαμερίσουμε το $\{1,\ldots,n\}$ σε ένα σύνολο μεγέθους k_1, σε ένα σύνολο μεγέθους k_2 και τέλος σε ένα σύνολο μεγέθους k_r;

Θεώρημα 4.3
Το πλήθος τρόπων να διαμερίσουμε ένα σύνολο με n στοιχεία σε r σύνολα με μεγέθη $k_1,\ldots,k_r$, με $k_1+\cdots+k_r=n$, όταν δε μας ενδιαφέρει η σειρά των στοιχείων μέσα στα σύνολα αυτά, είναι

$$\binom{n}{k_1,\ldots,k_r}=\frac{n!}{k_1!k_2!\cdots k_r!}. \tag{4.4}$$

Απόδειξη

Το πρώτο σύνολο μπορεί να επιλεγεί με

$$\binom{n}{k_1}=\frac{n!}{k_1!(n-k_1)!}$$

τρόπους. Μετά από την επιλογή του πρώτου συνόλου απομένουν $n-k_1$ στοιχεία αχρησιμοποίητα, άρα το δεύτερο σύνολο μπορεί να επιλεγεί με

$$\binom{n-k_1}{k_2}=\frac{(n-k_1)!}{k_2!(n-k_1-k_2)!}$$

τρόπους. Συνεχίζονας κατ' αυτόν τον τρόπο παίρνουμε ότι η επιλογή του προτελευταίου συνόλου (με k_{r-1} στοιχεία) μπορεί να γίνει με

$$\frac{(n-k_1-\cdots-k_{r-2})!}{k_{r-1}!(n-k_1-\cdots-k_{r-1})!}=\frac{(n-k_1-\cdots-k_{r-2})!}{k_{r-1}!k_r!}$$

τρόπους. Επίσης, αφού έχουν επιλεγεί τα $r-1$ πρώτα σύνολα δεν υπάρχει πλέον καμιά επιλογή να γίνει αφου τα υπόλοιπα k_r στοιχεία που απομένουν ακόμη αχρησιμοποίητα αναγκαστικά πάνε στο τελευταίο σύνολο που πρέπει να επιλέξουμε.

Έτσι πολλαπλασιάζοντας τις δυνατότητες επιλογών μας για τα πρώτα $r-1$ σύνολα, και κάνοντας τις απλοποιήσεις παίρνουμε τον τύπο (4.4).
■

Το σύμβολο $\binom{n}{k_1,\ldots,k_r}$ ονομάζεται *πολυωνυμικός συντελεστής* (κατ' αναλογία με τα $\binom{n}{k}$ που ονομάζονται *διωνυμικοί συντελεστές*). Παρατηρήστε επίσης ότι

$$\binom{n}{k,n-k}=\binom{n}{k}=\binom{n}{n-k}.$$

Παρατήρηση 4.1
Ο πολυωνυμικός συντελεστής $\binom{n}{k_1,\ldots,k_r}$ δεν αλλάζει αν τα $k_1,\ldots,k_r$ αντικατασταθούν από μια μετάθεσή τους (αν αλλάξει δηλ. απλώς η σειρά τους).

Παρατήρηση 4.2
Πρέπει να τονίσουμε εδώ ότι, αν και δε μας ενδιαφέρει η εσωτερική σειρά των συνόλων των στοιχείων που επιλέγουμε, η σειρά των ίδιων των συνόλων είναι προκαθορισμένη. Αυτό είναι ίσως φανερό όταν όλα τα $k_1,k_2,\ldots,k_m$ είναι μεταξύ τους διαφορετικά αλλά δημιουργεί κάποια σύγχυση όταν μερικά από αυτά είναι μεταξύ τους ίσα. Μια ακραία περίπτωση αυτού είναι όταν όλα είναι ίδια. Για παράδειγμα, ο πολυωνυμικός συντελεστής

$$\binom{9}{3,3,3}$$

μετράει με πόσους τρόπους μπορούμε να χωρίσουμε τους αριθμούς $1, 2, \ldots, 9$ *σε τρείς ομάδες. Αν δύο τρόποι διαφέρουν μόνο ως προς τον εσωτερικό τρόπο γραφής της κάθε ομάδας τότε δε θεωρούνται διαφορετικοί. Έτσι οι τρόποι*

$$\{1,2,3\},\{4,5,6\},\{7,8,9\} \text{ και } \{3,2,1\},\{4,5,6\},\{7,8,9\}$$

θεωρούνται ίδιοι και μετράνε ως ένα. Αν όμως δύο τρόποι διαφέρουν ως προς τον τρόπο γραφής των ομάδων τότε μετράνε ως διαφορετικοί. Οι τρόποι, π.χ.,

$$\{1,2,3\},\{4,5,6\},\{7,8,9\} \text{ και } \{4,5,6\},\{1,2,3\},\{7,8,9\}$$

μετράνε ως διαφορετικοί τρόποι.

✏ **4.11**
Έχουμε 10 αριθμημένες μπάλες και τρία κουτιά με χωρητικότητες 5, 3 και 2 μπάλες. Με πόσους τρόπους μπορούμε να βάλουμε τις μπάλες στα κουτιά; (Δεν υπάρχει εσωτερική σειρά στα κουτιά αλλά τα κουτιά είναι μεταξύ τους διακεκριμένα.)

✏ **4.12**
Με πόσους τρόπους μπορούμε να τοποθετήσουμε 12 αριθμημένες μπάλες σε 4 όμοια (μη αριθμημένα) κουτιά χωρητικότητας 3 το καθένα;

✏ **4.13**
Με πόσους τρόπους μπορούμε να διατάξουμε 5 γράμματα Α, 3 γράμματα Β και 4 γράμματα Γ; Εκφράστε την απάντησή σας σαν ένα πολυωνυμικό συντελεστή.

4.3 Το Διωνυμικό Θεώρημα

Το Διωνυμικό Θεώρημα (Θεώρημα 4.4 είναι ένα ισχυρότατο εργαλείο για υπολογισμούς που αναφέρονται σε ποσότητες με διωνυμικούς συντελεστές. Είναι επίσης η πρώτη σύνδεση των συνδυαστικών ποσοτήτων που συναντάμε με αλγεβρικές μεθόδους. Αργότερα θα δούμε και τις γεννήτριες συναρτήσεις ακολουθιών σα μια φυσική επέκταση της μεθόδου.

Θεώρημα 4.4
Για κάθε $a, b \in \mathbb{R}$*, και ακέραιο* $n \geq 0$ *ισχύει*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}. \tag{4.5}$$

Απόδειξη

Το αριστερό μέλος είναι ένα γινόμενο n παραγόντων ίσων με $(a+b)$. Όταν κάνουμε όλες τις πράξεις, όταν δηλ. εφαρμόσουμε την επιμεριστική ιδιότητα, αυτό που κάνουμε είναι ότι σχηματίζουμε όλα τα γινόμενα που μπορούμε να φτιάξουμε διαλέγοντας ένα προσθετέο από κάθε παράγοντα (δείτε και Παράδειγμα 3.7) και τα προσθέτουμε, μαζεύοντας μαζί ίδια μονώνυμα.

Είναι φανερό ότι, εφόσον οι προσθετέοι από κάθε παράδειγμα είναι a ή b και το πλήθος των παραγόντων είναι n, όλα τα μονώνυμα που θα εμφανιστούν είναι της μορφής

$$a^k b^{n-k},\ (0 \leq k \leq n).$$

Το μονώνυμο αυτό εμφανίζεται οποτεδήποτε έχουμε επιλέξει το a από ακριβώς k από τους παράγοντες. Αλλά αυτό συμβαίνει με ακριβώς τόσους τρόπους όσοι είναι οι τρόποι να επιλεγούν k παράγοντες από τους n, δηλ. $\binom{n}{k}$, και αυτό ακριβώς είναι το περιεχόμενο του θεωρήματος.
■

✏ **4.14**
Ποιο είναι το ανάπτυγμα του $(1+x)^5$ *σε δυνάμεις του* x*;*

Το Διωνυμικό Θεώρημα (Θεώρημα 4.4) έχει πολλές εφαρμογές σε υπολογισμούς αθροισμάτων.

Παράδειγμα 4.4
Θέτοντας $a=b=1$ *στην* (4.5) *παίρνουμε την ταυτότητα (δείτε και την Άσκηση 3.36)*

$$2^n=\sum_{k=0}^{n}\binom{n}{k}.$$

Παράδειγμα 4.5
Θέτοντας $a=1, b=-1$ *στην* (4.5) *και χωρίζοντας τους αρνητικούς από τους θετικούς όρους παίρνουμε ότι για κάθε* n *το άθροισμα των διωνυμικών συντελεστών* $\binom{n}{k}$ *για* k *άρτιο είναι ίσο με το άθροισμα για* k *περιττό*

$$\sum_{\substack{0\le k\le n\\ k\ \pi\varepsilon\rho\iota\tau\tau o}}\binom{n}{k}=\sum_{\substack{0\le k\le n\\ k\alpha\rho\tau\iota o}}\binom{n}{k}. \tag{4.6}$$

Αυτό είναι φανερό όταν το n *είναι περιττό, μια και τότε οι διωνυμικοί συντελεστές με άρτιο* k *βρίσκονται σε ένα προς ένα αντιστοιχία με τους συντελεστές με περιττό* k *(αφού ισχύει πάντα* $\binom{n}{k}=\binom{n}{n-k}$*–δείτε και Άσκηση 3.37), αλλά δεν είναι εξίσου εύκολο για άρτιο* k*.*

Παράδειγμα 4.6
Θέτουμε $a=x, b=1$ *στην* (4.5) *και παραγωγίζουμε τη σχέση που προκύπτει ως προς* x*. Παίρνουμε έτσι*

$$n(1+x)^{n-1}=\sum_{k=1}^{n}k\binom{n}{k}x^{k-1}.$$

Θέτοντας τώρα $x=1$ *παίρνουμε τη σχέση*

$$\sum_{k=1}^{n}k\binom{n}{k}=n2^{n-1}.$$

✏ **4.15**
Υπολογίστε το άθροισμα $\sum_{k=0}^{n}2^k\binom{n}{k}$*.*

✏ **4.16**
Υπολογίστε το άθροισμα $\sum_{k=2}^{n}k(k-1)\binom{n}{k}$*.*

✏ **4.17**
Έστω ότι έχουμε δύο συναρτήσεις

$$a(x)=a_{-N}x^{-N}+a_{-N+1}x^{-N+1}+\cdots+a_0+a_1x+\cdots a_Nx^N$$

και

$$b(x)=b_{-N}x^{-N}+b_{-N+1}x^{-N+1}+\cdots+b_0+b_1x+\cdots b_Nx^N$$

όπου τα a_j *και* b_j *είναι πραγματικοί αριθμοί. Μια τέτοια συνάρτηση (δεν ορίζεται στο* 0*) ονομάζεται* πολυώνυμο Laurent *και η διαφορά του από τα συνήθη πολυώνυμα είναι ότι έχουμε και αρνητικούς εκθέτες. Αποδεικνύεται ότι οι συντελεστές* a_j *καθορίζονται από τη συνάρτηση* $a(x)$*, δε μπορεί δηλ. η ίδια συνάρτηση να γραφτεί με διαφορετικούς συντελεστές.*

Αν γράψουμε $c(x)=a(x)b(x)$ *δείξτε ότι και η συνάρτηση* $c(x)$ *είναι πολυώνυμο Laurent και ότι οι συντελεστές της δίνονται από τον τύπο*

$$c_s=\sum_{\max\{-N,s-N\}}^{\min\{N,N-s\}}a_kb_{s-k},$$

για $-2N\le s\le 2N$*.*

✏ **4.18**
Θέτοντας $a = x, b = 1/x$ και $2n$ στη θέση του n στην (4.5) δείξτε την ταυτότητα

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2,$$

εξετάζοντας το συντελεστή του σταθερού όρου και χρησιμοποιώντας και την Άσκηση 4.17.

✏ **4.19**
Ποιος ο συντελεστής του x^3y^5 στο ανάπτυγμα του $(1 + x + y)^{12}$; Εκφράστε την απάντησή σας με πολυωνυμικούς συντελεστές. (Δείτε την §4.2.)

Παράδειγμα 4.7
Σε αυτό το παράδειγμα υπολογίζουμε το άθροισμα

$$\sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k}.$$

Και πάλι χρησιμοποιούμε το διωνυμικό θεώρημα. Κατ' αναλογία με το Παράδειγμα 4.6 στο οποίο παραγωγίσαμε ως προς x το διωνυμικό θεώρημα στη μορφή

$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

ώστε να εμφανίσουμε ένα παράγοντα k μπροστά από το διωνυμικό συντελεστή $\binom{n}{k}$ στο δεξί μέλος, εδώ θέλουμε να εμφανίσουμε ένα παράγοντα $1/(k + 1)$ οπότε το φυσιολογικό είναι να ολοκληρώσουμε. Έστω λοιπόν

$$f(x) = \sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k} x^k.$$

Εμάς μας ενδιαφέρει να βρούμε το $f(1)$ αλλά θα βρούμε τελικά ένα τύπο για τη συνάρτηση $f(x)$ πριν θέσουμε $x = 1$. Πολλαπλασιάζουμε την προηγούμενη ισότητα με x και έπειτα την παραγωγίζουμε ως προς x για να πάρουμε

$$(xf(x))' = \sum_{k=0}^{n} \binom{n}{k} x^k = (1 + x)^n$$

από την οποία, με ολοκλήρωση, προκύπτει ότι υπάρχει μια σταθερά C τέτοια ώστε

$$xf(x) = \int (1 + x)^n \, dx + C$$

ή

$$xf(x) = \frac{(1 + x)^{n+1}}{n + 1} + C.$$

Θέτοντας $x = 0$ προκύπτει ότι $C = -1/(n + 1)$ οπότε

$$xf(x) = \frac{(1 + x)^{n+1} - 1}{n + 1}$$

και με $x = 1$ παίρνουμε $f(1) = \frac{2^n-1}{n+1}$

4.4 Συνδυαστικές αποδείξεις ταυτοτήτων

Σε αυτή την παράγραφο θα δούμε πώς μπορούμε πολλές φορές να αποδεικνύουμε ταυτότητες χωρίς ιδιαίτερες πράξεις, απλά ερμηνεύοντας το αριστερό και το δεξί μέλος με συνδυαστικό τρόπο και παρατηρώντας ότι απαριθμούν τα ίδια αντικείμενα (άρα είναι και ίσα). Αυτή η τεχνική ονομάζεται και *διπλό μέτρημα* μια και μετράμε τα ίδια αντικείμενα δύο φορές, άρα τα δύο αποτελέσματα είναι ίσα.

Παράδειγμα 4.8
(Τρίγωνο του Pascal) *Δείξτε την ταυτότητα*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \tag{4.7}$$

Το αριστερό μέλος μετράει τα k-μελή υποσύνολα του $[n] = \{1, \ldots, n\}$. Αυτά όμως είναι δυο κατηγοριών: αυτά που περιέχουν το στοιχείο n και τα υπόλοιπα. Το πλήθος αυτών που περιέχουν το n είναι $\binom{n-1}{k-1}$ αφού κάθε ένα από αυτά τα k-μελή υποσύνολα καθορίζεται μονοσήμαντα από την τομή του με το σύνολο $[n-1] = \{1, \ldots, n-1\}$ που έχει μέγεθος $k-1$. Τα υπόλοιπα υποσύνολα επίσης καθορίζονται μονοσήμαντα από την τομή τους με το $[n-1]$, μόνο που αυτή τώρα έχει μέγεθος k, άρα το πλήθος τους είναι $\binom{n-1}{k}$.

Παράδειγμα 4.9
Σε μια συγκέντρωση ο αριθμός των καλεσμένων που ανταλλάσσουν περιττές σε πλήθος χειραψίες είναι άρτιος.

Έστω $P_1, \ldots, P_n$ οι καλεσμένοι. Θεωρούμε το σύνολο των ζευγών (P_i, P_j) τέτοια ώστε ο P_i χαιρετάει τον P_j, και ας είναι x_i ο αριθμός των χειραψιών που ανταλλάσσει ο P_i και y ο συνολικός αριθμός χειραψιών που ανταλλάσονται. Το πλήθος των ζευγών (P_i, P_j) ισούται, από τη μια μεριά, με $\sum_{i=1}^{n} x_i$, και, από την άλλη, με $2y$, αφού σε κάθε χειραψία αντιστοιχούν ακριβώς δύο ζευγάρια (P_i, P_j) και (P_j, P_i). Έτσι έχουμε

$$2y = \sum_{i=1}^{n} x_i$$

άρα το πλήθος των περιττών x_i είναι αναγκαστικά άρτιο.

Παράδειγμα 4.10
Για $n_1, n_2 \geq 0$ ισχύει

$$\sum_{k=0}^{m} \binom{n_1}{k}\binom{n_2}{m-k} = \binom{n_1+n_2}{m}, \quad (m \leq \min\{n_1, n_2\}).$$

Δεξιά μετράμε τα υποσύνολα μεγέθους m του $[n_1+n_2]$. Βάφουμε τα n_1 αντικείμενα άσπρα και τα άλλα μαύρα. Τα υποσύνολα μεγέθους m που μας ενδιαφέρουν χωρίζονται στις $m+1$ σε πλήθος κατηγορίες C_k, $k = 0, \ldots, m$. Η κατηγορία C_k περιλαμβάνει όλα τα m-μελή υποσύνολα του $[n_1+n_2]$ που περιέχουν ακριβώς k άσπρα. Προφανώς έχουμε $|C_k| = \binom{n_1}{k}\binom{n_2}{m-k}$ αφού για να φτιάξουμε ένα υποσύνολα κατηγορίας C_k πρέπει να επιλέξουμε k άσπρα και τα υπόλοιπα $n-k$ μαύρα. Άρα το αριστερό μέλος της ισότητας είναι ίσο με $\sum_{k=0}^{m} |C_k|$.

Παράδειγμα 4.11
Για κάθε $n \geq 2$ ισχύει:

$$\binom{2n}{2} = 2\binom{n}{2} + n^2.$$

Αριστερά μετράμε διμελή υποσύνολα του $[2n]$. Έστω ότι χρωματίζουμε n από τα $2n$ αντικείμενα σε άσπρα και τα άλλα μαύρα. Τα διμελή υποσύνολα του $[2n]$ είναι τριών τύπων: (Α) δύο στοιχεία άσπρα, (Β) δύο στοιχεία μαύρα, (Γ) ένα άσπρο κι ένα μαύρο. Τα υποσύνολα τύπου (Α) είναι $\binom{n}{2}$ σε πλήθος αφού διαλέγουμε δύο από τα n άσπρα. Τόσα είναι και τα υποσύνολα τύπου (Β). Τα σύνολα τύπου (Γ) είναι σε πλήθος $n \cdot n$, μια και πρέπει να διαλέξουμε ένα από n άσπρα και ένα από n μαύρα. Το σύνολο για τις τρεις κατηγορίες συνόλων εμφανίζεται στο δεξί μέλος.

Παράδειγμα 4.12
Δείξτε ότι

$$n2^{n-1} = \sum_{k=1}^{n} k\binom{n}{k} \tag{4.8}$$

(δείτε επίσης το Παράδειγμα 4.6) αριθμώντας με δύο διαφορετικούς τρόπους τα ζεύγη (x, M) τέτοια ώστε $x \in M \subseteq [n]$.

Υπάρχουν $\binom{n}{k}$ σύνολα $M \subseteq [n]$ με μέγεθος k, και για κάθε ένα από αυτά μπορούμε να επιλέξουμε ως x οποιοδήποτε από τα k στοιχεία του, άρα το πλήθος των ζευγών (x, M) τέτοια ώστε $x \in M \subseteq [n]$ ισούται με το δεξί μέλος της (4.8).

Όμως τα ζεύγη αυτά μπορούν να αριθμηθούν επιλέγοντας πρώτα το x και μετά επιλέγοντας τα υπόλοιπα στοιχεία του M, το σύνολο δηλ. $M \setminus \{x\}$. Όμως όλα τα σημεία του $[n]$ εκτός το x συμμετέχουν στον καθορισμό του $M \setminus \{x\}$, και άρα οι δυνατότητες γι' αυτό είναι 2^{n-1}, άρα οι δυνατότητες για τα ζεύγη είναι $n2^{n-1}$, που είναι το αριστερό μέλος.

✏ **4.20**
Αποδείξτε με συνδυαστικό επιχείρημα ότι αν $0 \le i \le k \le n$ τότε ισχύει

$$\binom{n}{i}\binom{n-i}{k-i} = \binom{k}{i}\binom{n}{k}.$$

✏ **4.21**
Αποδείξτε με συνδυαστικό επιχείρημα την ταυτότητα

$$\binom{n}{k} = \sum_{i=k}^{n} \binom{i-1}{k-1}.$$

Πόσα υποσύνολα του $[n]$ μεγέθους k υπάρχουν τ.ώ. το μεγαλύτερο στοιχείο τους να είναι το i;

✏ **4.22**
Αν $n, m, k_1, \ldots, k_m$ είναι μη αρνητικοί ακέραιοι τ.ώ. $k_1 + \cdots + k_m = n$ δείξτε με συνδυαστικό επιχείρημα ότι ισχύει

$$\binom{n}{k_1, k_2, \ldots, k_m} = \sum_{i=1}^{m} \binom{n-1}{k_1, \ldots, k_{i-1}, (k_i - 1), k_{i+1}, \ldots, k_m}.$$

✏ **4.23**
Αποδείξτε με συνδυαστικό επιχείρημα την ταυτότητα

$$\binom{0}{m} + \binom{1}{m} + \cdots + \binom{n}{m} = \binom{n+1}{m+1}$$

όπου $0 \le m \le n$. (Θυμηθείτε ότι οι διωνυμικοί συντελεστές $\binom{a}{b}$ με $a < b$ ισούνται με 0.)

4.5 Επαναληπτικές ασκήσεις Κεφαλαίου

✏ **4.24**
Με πόσους τρόπους μπορούμε να μοιράσουμε 21 διαφορετικά βιβλία στα άτομα Α, Β και Γ, ούτως ώστε οι Α και Β μαζί να πάρουν διπλάσια βιβλία από τον Γ;

✏ **4.25**
Μια ομάδα 20 ατόμων θέλει να φτιάξει τρεις, ξένες μεταξύ τους, επιτροπές με 6, 5 και 4 άτομα η κάθε μία. (Μέσα σε κάθε επιτροπή δεν υπάρχουν χωριστά αξιώματα–τα μέλη τους είναι ισοδύναμα.) Με πόσους τρόπους μπορεί να γίνει αυτό;

✏ **4.26**
Υπολογίστε το άθροισμα

$$\sum_{k=1}^{n} k^2 \binom{n}{k}.$$

✏ **4.27**
Δείξτε ότι, για $n \geq 1$ ισχύει

$$\binom{2n+2}{n+1} = \binom{2n}{n+1} + 2\binom{2n}{n} + \binom{2n}{n-1}. \tag{4.9}$$

4.6 Video Κεφαλαίου

4.1
Συνδυασμοί k από n με επανάθεση. (video και συνοδευτικές ασκήσεις, 14:35 λεπτά).

4.2
Το διωνυμικό θεώρημα και κάποιες εφαρμογές. (video και συνοδευτικές ασκήσεις, 19:09 λεπτά).

Βιβλιογραφία Κεφαλαίου

[1] Peter J Cameron. *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, 1994.

[2] Ronald L Graham, Donald E Knuth, and Oren Patashnik. *Concrete Mathematics*. 1994.

[3] Chung Laung Liu and CL Liu. *Elements of discrete mathematics*. McGraw-Hill New York, 1985.

[4] Richard P Stanley. *Enumerative combinatorics*. 1986.

Κεφάλαιο 5

Εισαγωγή στη θεωρία γραφημάτων

Κύριες βιβλιογραφικές αναφορές για αυτό το Κεφάλαιο είναι οι C. L. Liu and C. Liu 1985, Cameron 1994, Diestel 2005 και Stanley 1986.

5.1 Απλά γραφήματα

Ένα γράφημα (μερικές φορές στην ελληνική βιβλιογραφία γίνεται λόγος και για ένα γράφο) είναι ο βασικότερος, παραστατικότερος και πλέον εύχρηστος γενικός τρόπος στα Μαθηματικά (αλλά και στις Επιστήμες γενικότερα) να παραστήσει κανείς πληροφορία συνδεσμολογίας, να περιγράψει δηλ. μια ομάδα αντικειμένων μερικά από τα οποία συνδέονται μεταξύ τους, και ενδεχομένως και πληροφορίες για τη συνδεσμολογία.

Ορισμός 5.1
(Απλό γράφημα) *Ενα* απλό γράφημα $G = (V, E)$ *αποτελείται από ένα σύνολο κορυφών* V *και ένα σύνολο ακμών* E*, το οποίο είναι ένα σύνολο από* δισύνολα *του* V*. Γράφουμε επίσης* $V = V(G)$ *και* $E = E(G)$ *για τα σύνολα κορυφών και ακμών του γραφήματος* G*.*

Μια ακμή ανάμεσα σε δύο κορυφές u και v αντιπροσωπεύει κάποια έννοια σύνδεσης των δύο κορυφών. Συνηθίζουμε να παριστάνουμε ένα γράφημα αντιστοιχώντας ένα σημείο του επιπέδου σε κάθε κορυφή και τραβώντας μια γραμμή που ενώνει δυο κορυφές αν και μόνο αν αυτές ενώνονται με μια ακμή στο G.

Επισημαίνουμε εδώ ότι αυτή η γραφική παράσταση ενός γραφήματος έχει εποπτική μόνο σημασία. Υπάρχουν γραφήματα στα οποία δε χρησιμοποιούμε ποτέ κάποια γραφική παράσταση (συνήθως λόγω μεγέθους) και τα γραφήματα που μπορούν να παρασταθούν γραφικά με διάφορους τρόπους.

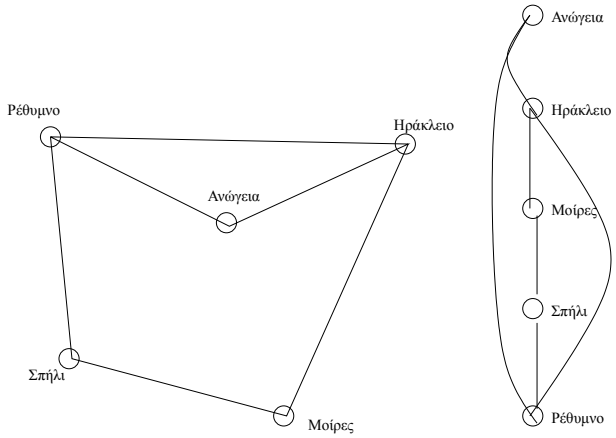
Για παράδειγμα, στο Σχήμα 5.1 δείχνουμε με δύο διαφορετικούς τρόπους το ίδιο γράφημα που σκοπό έχει να δείξει την οδική συνδεσμολογία ανάμεσα σε πέντε πόλεις της Κρήτης. Η ύπαρξη μιας ακμής ανάμεσα σε δύο κορυφές (πόλεις) υποδηλώνει την ύπαρξη ενός δρόμου. Το σύνολο κορυφών σε αυτό το γράφημα είναι το

$$V = \{ \text{Ηράκλειο, Ρέθυμνο, Ανώγεια, Μοίρες, Σπήλι} \}$$

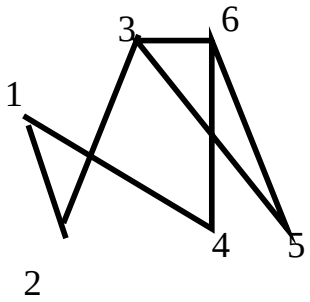
ενώ το σύνολο ακμών είναι το

$$E = \{ \{ \text{Ηράκλειο, Ρέθυμνο} \}, \{ \text{Ηράκλειο, Ανώγεια} \}, \{ \text{Ανώγεια, Ρέθυμνο} \}, \{ \text{Ρέθυμνο, Σπήλι} \}, \{ \text{Σπήλι, Μοίρες} \}, \{ \text{Μοίρες, Ηράκλειο} \} \}.$$

Στην αριστερή γραφική παράσταση του γραφήματος έχουμε ζωγραφίσει τις πόλεις σε τέτοια θέση ώστε η σχετική τους θέση να μοιάζει με αυτή που έχουν πάνω στο χάρτη, ενώ δεξιά έχουμε ζωγραφίσει το ίδιο γράφημα βάζοντας απλά όλες τις πόλεις τη μια κάτω από την άλλη σε αλφαβητική σειρά. Τονίζουμε ξανά ότι και τα δύο σχέδια παριστάνουν το ίδιο γράφημα.



Σχήμα 5.1: Κάποιες πόλεις στην Κρήτη και οδικές συνδέσεις ως γράφημα



Σχήμα 5.2: Ενα απλό γράφημα με 6 κορυφές και 7 ακμές

Παράδειγμα 5.1
Συνήθως τα ονόματα που επιλέγουμε για τις κορυφές είναι απλά αριθμοί. Ένα τυπικό γράφημα είναι π.χ. το γράφημα του Σχήματος 5.2 που έχει σύνολο κορυφών το

$$V = \{1, 2, 3, 4, 5, 6\}$$

και σύνολο ακμών το

$$E = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 5\}, \{3, 6\}, \{4, 6\}, \{5, 6\}\}.$$

✏ **5.1**
Δύο απλά γραφήματα $G_1 = (V, E)$ και $G_2 = (V, E_2)$ με το ίδιο σύνολο κορυφών λέγονται συμπληρωματικά αν $E_1 \cap E_2 = \emptyset$ και η ένωση $E_1 \cup E_2$ είναι όλα τα διμελή υποσύνολα του V. Με άλλα λόγια δύο κορυφές του V συνδέονται με ακμή στο G_1 αν και μόνο αν δε συνδέονται στο G_2.

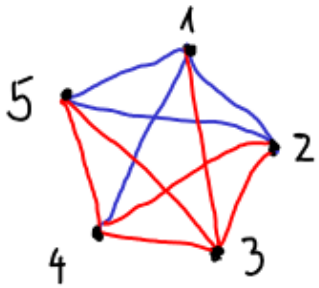
Δείτε το Σχήμα 5.3 για παράδειγμα.

Βρείτε το συμπληρωματικό γράφημα αυτού που παρουσιάζεται στο Παράδειγμα 5.1.

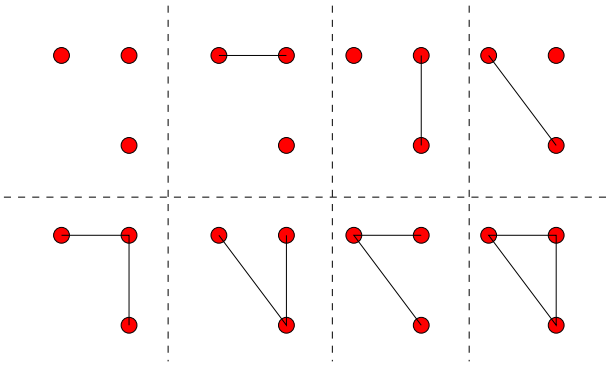
Παράδειγμα 5.2
Στο Σχήμα 5.4 δείχνουμε όλα τα διαφορετικά απλά γραφήματα με 3 κορυφές.

✏ **5.2**
Πόσα διαφορετικά γραφήματα υπάρχουν με n κορυφές; Πόσα με n κορυφές και k ακμές; ($0 \leq k \leq n$)

Αν δυο κορυφές u και v ενώνονται στο G (δηλ. αν $\{u, v\} \in E$) θα γράφουμε συνήθως $u \sim v$ ή και $u \overset{G}{\sim} v$ αν θέλουμε να τονίσουμε για ποιο γράφημα μιλάμε. Ομοίως θα γράφουμε $e_1 \sim e_2$ για δύο ακμές e_1 και e_2 αν αυτές μοιράζονται μια από τις δυό τους κορυφές.



Σχήμα 5.3: Εδώ βλέπουμε δύο συμπληρωματικά γραφήματα με κοινό σύνολο κορυφών $V = \{1, 2, 3, 4, 5\}$. Τα δύο γραφήματα είναι αυτό με τις μπλε και αυτό με τις κόκκινες ακμές. Κάθε δυνατή ακμή ανάμεσα σε στοιχεία του V είναι χρωματισμένη είτε μπλε είτε κόκκινη.



Σχήμα 5.4: Τα διαφορετικά απλά γραφήματα με 3 κορυφές

Ορισμός 5.2
(Γειτονικές κορυφές και ακμές, γειτονιές) *Δύο κορυφές που συνδέονται με ακμή (αντ. ακμές που έχουν μια κοινή κορυφή) θα λέγονται* γειτονικές *ή* γείτονες *και το σύνολο των γειτόνων μιας κορυφής (αντ. ακμής) u θα λέγεται η* γειτονιά *του u και θα συμβολίζεται συνήθως με $N(u)$.*

Δείτε το Σχήμα 5.5 για παράδειγμα.

Παράδειγμα 5.3
Στο γράφημα του Σχήματος 5.2 έχουμε

$$N(1) = \{2, 4\},\ N(2) = \{1, 3\},\ N(3) = \{2, 5, 6\},\ N(4) = \{1, 6\},\ N(5) = \{3, 6\},\ N(6) = \{3, 4, 5\}.$$

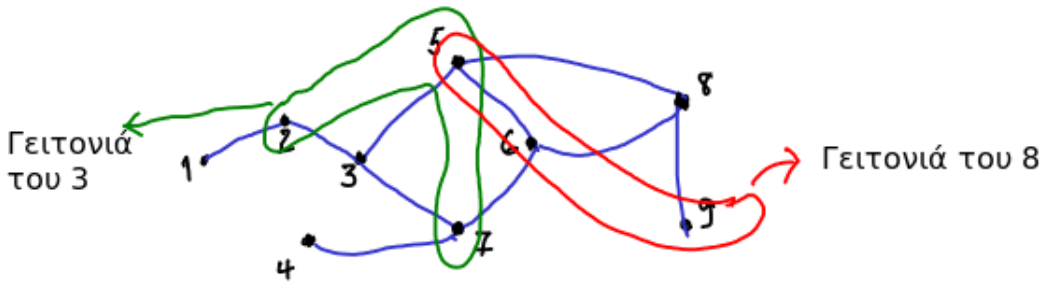
Η γειτονιά της ακμής $\{3, 6\}$ είναι το σύνολο ακμών

$$N((3, 6)) = \{\{2, 3\}, \{3, 5\}, \{4, 6\}, \{4, 5\}, \{3, 6\}\}.$$

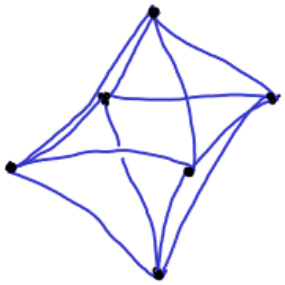
Παρατηρήστε ότι μια ακμή είναι πάντα γείτονας του εαυτού της σύμφωνα με τον ορισμό που έχουμε δώσει, ενώ μια κορυφή ποτέ δε γειτονεύει με τον εαυτό της σε ένα απλό γράφημα (αυτό αλλάζει αργότερα όταν θα εξετάζουμε γενικότερα γραφήματα).

Ορισμός 5.3
(Βαθμός κορυφής, ακμής. Κανονικό γράφημα.) Βαθμός *μιας κορυφής $u \in V$ (θα συμβολίζεται με* $\deg u$*) λέγεται το πλήθος των ακμών που έχουν την u ως άκρο τους. Δηλ.* $\deg u = |N(u)|$. *Ομοίως ορίζεται ο βαθμός μιας ακμής.*

Κανονικό *ονομάζεται ένα γράφημα όταν όλες οι κορυφές του έχουν τον ίδιο βαθμό. Αν ο κοινός αυτός βαθμός είναι r τότε λέγεται r-κανονικό.*



Σχήμα 5.5: Στο γράφημα αυτό φαίνεται με πράσινο χρώμα η γειτονιά της κορυφής 3 (οι κορυφές 2, 5, 7) και με κόκκινο χρώμα η γειτονιά της κορυφής 8 (οι κορυφές 5, 6, 9)



Σχήμα 5.6: Ένα κανονικό γράφημα βαθμού 4 με 6 κορυφές

Δείτε το Σχήμα 5.6 για παράδειγμα ενός κανονικού γραφήματος.

Παράδειγμα 5.4
Στο Σχήμα 5.2, αν σβήσουμε την ακμή $\{3, 6\}$, όλες οι κορυφές έχουν βαθμό 2, άρα είναι το γράφημα αυτό 2-κανονικό. Στο Σχήμα 5.1 ο βαθμός των κορυφών Ηράκλειο και Ρέθυμνο είναι 3 και των άλλων κορυφών είναι 2.

✏ **5.3**
Γίνεται σε ένα γράφημα όλες οι κορυφές να έχουν διαφορετικό βαθμό;
Οι δυνατές τιμές για το βαθμό μιας κορυφής σε ένα γράφημα με n κορυφές είναι $0, 1, \ldots, n-1$. Μπορούμε να έχουμε κορυφή βαθμού 0 και κορυφή βαθμού $n-1$ ταυτόχρονα;

✏ **5.4**
Δείξτε ότι σε ένα γράφημα $G = (V, E)$ το άθροισμα των βαθμών όλων των κορυφών ισούται με $2|E|$.

✏ **5.5**
Πόσες ακμές έχει ένα r-κανονικό γράφημα με n κορυφές; Υπάρχει 3-κανονικό γράφημα με 7 κορυφές;
Άσκηση 5.4.

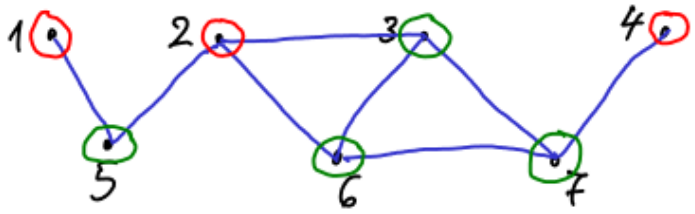
✏ **5.6**
Δείξτε ότι σε οποιοδήποτε γράφημα το πλήθος κορυφών με περιττό βαθμό είναι άρτιο.

✏ **5.7**
Αν $n > 0$ δείξτε ότι υπάρχει n-κανονικό γράφημα με $2n$ κορυφές.

✏ **5.8**
Ένα σύνολο κορυφών ενός γραφήματος λέγεται **ανεξάρτητο** *αν κάθε δύο κορυφές του δε συνδέεονται με ακμή. Επίσης, ένα σύνολο κορυφών λέγεται* **κάλυμμα** *αν κάθε ακμή του γραφήματος περιέχει κάποια από τις κορυφές αυτές.*

Δείξτε ότι σ' ένα γράφημα $G = (V, E)$ το σύνολο κορυφών $A \subseteq V$ είναι ανεξάρτητο αν και μόνο αν το σύνολο κορυφών $V \setminus A$ είναι κάλυμμα.

Δείτε το Σχήμα 5.7 για παράδειγμα.



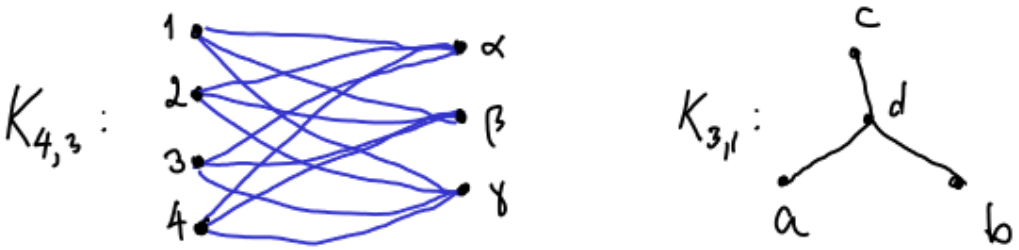
Σχήμα 5.7: Στο γράφημα αυτό οι κόκκινες κορυφές αποτελούν ανεξάρτητο σύνολο και το συμπλήρωμά τους, οι πράσινες κορυφές, αποτελούν κάλυμμα

5.2 Μερικά ειδικά γραφήματα

Το κενό γράφημα με n κορυφές έχει σύνολο κορυφών $[n] = \{1, \ldots, n\}$ και σύνολο ακμών $E = \emptyset$. Το συμβολίζουμε με E_n.

Το πλήρες γράφημα με n κορυφές έχει σύνολο κορυφών $[n]$ και όλες τις δυνατές ακμές, δηλ. $E =$ όλα τα διμελή υποσύνολα του $[n]$. Συμβολίζεται με K_n και έχει $\binom{n}{2} = \frac{n(n-1)}{2}$ ακμές. Το αριστερό γράφημα στο Σχ. 5.10 είναι το K_5.

Το πλήρες διμερές γράφημα με m και n κορυφές έχει σύνολο κορυφών το $V = A \cup B$, με $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$, και $a_i \sim b_j$, για κάθε $i = 1, \ldots, m$, $j = 1, \ldots, n$. Συμβολίζεται με $K_{m,n}$ και έχει $m \cdot n$ ακμές. Δείτε το Σχήμα 5.8 για παράδειγμα.



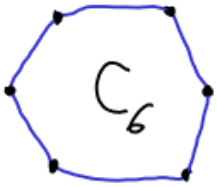
Σχήμα 5.8: Το πλήρες διμερές γράφημα $K_{4,3}$ με $A = \{1, 2, 3, 4\}, B = \{\alpha, \beta, \gamma\}$ και το πλήρες διμερές γράφημα $K_{3,1}$, ζωγραφισμένο με ασυνήθιστο τρόπο, με $A = \{a, b, c\}, B = \{d\}$.

Ο κύκλος με n κορυφές έχει σύνολο κορυφών το $[n]$ και $i \sim j$ αν και μόνο αν $|i - j| = 1$ ή $\{i, j\} = \{1, n\}$. Συμβολίζεται με C_n και έχει n ακμές. Δείτε το Σχήμα 5.9 για παράδειγμα.

5.3 Υπογραφήματα και ισομορφία

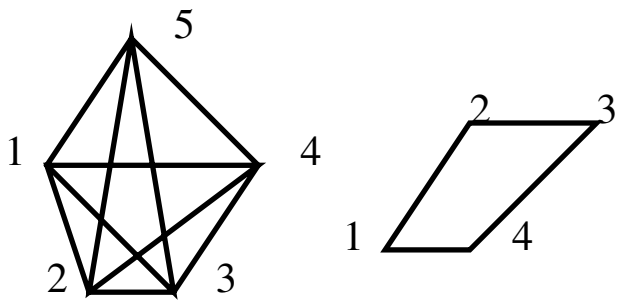
5.3.1 Υπογραφήματα

Ορισμός 5.4
(Υπογράφημα) *Ενα γράφημα $G' = (V', E')$ θα λέγεται* υπογράφημα *ενός γραφήματος $G = (V, E)$ αν $V' \subseteq V$ και $E' \subseteq E$.*



Σχήμα 5.9: Ο κύκλος C_6

Με άλλα λόγια, το G' είναι υπογράφημα του G αν μπορούμε να το πάρουμε από το G αφαιρώντας κάποιες κορυφές και κάποιες ακμές. Εννοείται εδώ ότι αν αποφασίσουμε να αφαιρέσουμε από το G μια κορυφή u αυτόματα διαγράφουμε και όλες τις ακμές που περιέχουν την u, μια και δεν έχουν πλέον «νόημα».



Σχήμα 5.10: Το δεξί γράφημα είναι υπογράφημα του αριστερού

Παράδειγμα 5.5
Στο Σχήμα 5.10 το γράφημα δεξιά είναι υπογράφημα του γραφήματος αριστερά. Παρατηρήστε ότι το γράφημα δεξιά είναι ζωγραφισμένο «διαφορετικά» απ' ότι το αντίστοιχό του αριστερά. Ας τονίσουμε εδώ ότι αυτό δεν έχει σημασία, μια και ένα γράφημα μπορεί να ζωγραφιστεί με πολλούς τρόπους στο επίπεδο. Αυτό που έχει σημασία είναι το ποια συνδεσμολογία (ποιες ακμές) υποδηλώνονται από το σχήμα. Από κει και πέρα είμαστε ελεύθεροι να επιλέξουμε να παραστήσουμε το γράφημα ως σχήμα με όποιο τρόπο προσφέρεται για τους σκοπούς μας.

✏ **5.9**
Πόσες ακμές έχει το πλήρες γράφημα K_n; Πόσα υπογραφήματα έχει το K_n;
Για το πρώτο ερώτημα, αφού υπάρχουν όλες οι δυνατές ακμές τότε για να καθορίσουμε μια ακμή αρκεί να προσδιορίσουμε το ζεύγος των κορυφών της. Για το δεύτερο ερώτημα, για να καθοριστεί ένα υπογράφημα πρέπει (α) να καθορίσουμε ποιο θα είναι το σύνολο των κορυφών του (ένα οποιοδήποτε υποσύνολο του $[n]$) και (β) αφού προσδιορίσουμε το ποιες είναι οι κορυφές του υπογραφήματος θα πρέπει να αποφασίσουμε το ποιες είναι οι ακμές του. Το πλήθος των επιλογών στο (β) εξαρτάται προφανώς από το πόσες κορυφές επιλέξαμε στο (α). Π.χ. αν στο βήμα (α) επιλέξαμε 5 κορυφές στο βήμα (β) έχουμε να διαλέξουμε ένα οποιοδήποτε υποσύνολο όλων των δυνατών ακμών, των οποίων το πλήθος είναι $\binom{5}{2}$.
Έτσι, η απάντηση στο τελευταίο είναι ένα άθροισμα (για όλα τα $k = 0, 1, \ldots, n$, όπου k συμβολίζει το πόσες κορυφές επιλέξαμε στο βήμα (α)) που μάλλον δεν απλοποιείται.

Μια ειδική κατηγορία υπογραφημάτων είναι τα λεγόμενα *επαγόμενα* υπογραφήματα, τα οποία προκύπτουν από ένα γράφημα διαγράφοντας απλώς ορισμένες κορυφές και χωρίς περιττές διαγραφές ακμών.

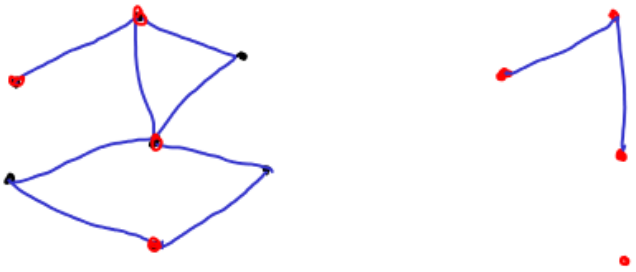
Ορισμός 5.5
Αν $V' \subseteq V$, τότε το υπογράφημα του $G = (V, E)$ που επάγεται *από το σύνολο κορυφών V' είναι το*

γράφημα $G' = (V', E')$*, με*

$$E' = \{e = \{u, v\} \in E : \quad u, v \in V'\}.$$

Δείτε το Σχήμα 5.11 για παράδειγμα.

Στο Σχήμα 5.10 το γράφημα δεξιά δεν είναι επαγόμενο υπογράφημα αφού λείπουν οι ακμές $\{2, 4\}$ και $\{1, 3\}$. Αν τις προσθέσουμε σε αυτό τότε γίνεται το υπογράφημα του αριστερού γραφήματος που επάγεται από το σύνολο κορυφών $V = \{1, 2, 3, 4\}$.



Σχήμα 5.11: Το γράφημα δεξιά είναι αυτό που επάγουν οι κόκκινες κορυφές στο γράφημα αριστερά

✏ **5.10**

Πόσα επαγόμενα υπογραφήματα έχει ένα γράφημα με n *κορυφές;*

Για ένα δεδομένο γράφημα G *ένα επαγόμενο υπογράφημά του είναι πλήρως καθορισμένο αν καθορίσουμε το ποιες είναι οι κορυφές του* G *που το επάγουν (σύνολο* V' *στον Ορισμό 5.5).*

5.3.2 Ισομορφία γραφημάτων

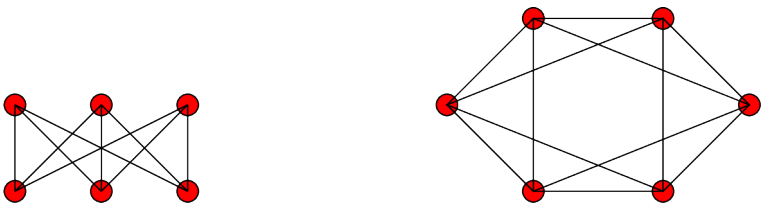
Ορισμός 5.6

Δύο γραφήματα $G = (V, E)$ *και* $G' = (V', E')$*, με ίδιο πλήθος κορυφών, λέγονται* ισόμορφα *ή* ισομορφικά *αν υπάρχει μια 1-1 και επί συνάρτηση* $f : V \to V'$ *τέτοια ώστε να έχουμε*

$$\forall u, v \in V : \left(u \overset{G}{\sim} v \iff f(u) \overset{G'}{\sim} f(v)\right). \tag{5.1}$$

Με άλλα λόγια, δυο γραφήματα λέγονται ισόμορφα αν μπορούμε να αντιστοιχίσουμε τις κορυφές τους 1-1 με τέτοιο τρόπο ώστε να διατηρείται η συνδεσμολογία.

Δείτε το Σχήμα 5.12 για παράδειγμα.



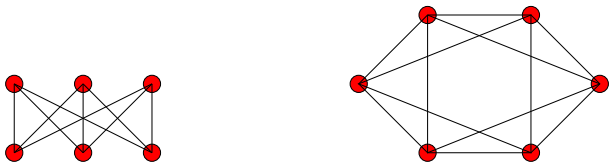
Σχήμα 5.12: Τα δύο γραφήματα είναι ισόμορφα με την αντιστοίχιση κορυφών (συνάρτηση f στον Ορισμό 5.6) $\alpha \to 1, \beta \to 2, \gamma \to 3, \delta \to 4, \epsilon \to 5$

✏ **5.11**

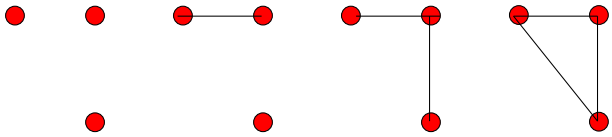
Δείξτε ότι η ισομορφία γραφημάτων είναι μια σχέση ισοδυναμίας. Δηλ. αν F*,* G *και* H *είναι απλά γραφήματα τότε:*

- Ανακλαστική ιδιότητα: F *είναι ισόμορφο με το* F*,*

- Συμμετρική ιδιότητα: *Αν το F είναι ισόμορφο με το G τότε και το G είναι ισόμορφο με το F, και*
- Μεταβατική ιδιότητα: *Αν F ισόμορφο με το G και G ισόμορφο με το H τότε και το F είναι ισόμορφο με το H.*



Σχήμα 5.13: Δείξτε ότι τα δύο γραφήματα δεν είναι ισόμορφα



Σχήμα 5.14: Τα μη-ισόμορφα γραφήματα με 3 κορυφές

Παράδειγμα 5.6
Στο Σχήμα 5.14 δείχνουμε όλα τα μη-ισόμορφα μεταξύ τους γραφήματα με 3 κορυφές. Κάθε άλλο δηλ. γράφημα με 3 κορυφές (φαίνονται στο Σχήμα 5.4) είναι ισόμορφο ακριβώς με ένα από τα 4 αυτά γραφήματα. Παρατηρήστε ότι το πλήθος τους είναι κατά πολύ μικρότερο του πλήθος όλων των γραφημάτων με 3 κορυφές, ισομόρφων μεταξύ τους ή όχι.

Η απεικόνιση f (που ονομάζεται *ισομορφισμός*) δεν είναι μοναδικά καθορισμένη και ούτε είναι συνήθως προφανής η ύπαρξή της. Π.χ. η απεικόνιση f από το γράφημα του Σχήματος 5.16 στο γράφημα του Σχήματος 6.1 που έχει

$$f(1) = 1, f(2) = 5, f(3) = 6, f(4) = 7, f(5) = 4, f(6) = 3, f(7) = 2,$$

είναι κι αυτή ένας ισομορφισμός από το πρώτο γράφημα στο δεύτερο.

Οσον αφορά τη θεωρία γραφημάτων, δύο ισόμορφα γραφήματα συνήθως δεν τα ξεχωρίζουμε μεταξύ τους. Π.χ. θα θεωρούμε ένα γράφημα G υπογράφημα ενός γραφήματος G' αν το G είναι ισόμορφο με κάποιο υπογράφημα του G'. Ετσι το γράφημα

$$\alpha - - - \beta - - - \gamma$$

(τρείς κορυφές και δύο ακμές) θεωρείται υπογράφημα του γραφήματος του Σχήματος 6.1 παρά το ότι το σύνολο κορυφών του δεν είναι καν υποσύνολο του συνόλου των κορυφών του Σχήματος 6.1.

✏ **5.12**
Δείξτε ότι κάθε απλό γράφημα G είναι ισομορφικό με κάποιο υπογράφημα του πλήρους γραφήματος K_n, όπου n είναι το πλήθος των κορυφών του G.

✏ **5.13**
Δείξτε ότι δύο ισομορφικά γραφήματα έχουν το ίδιο πλήθος ακμών.

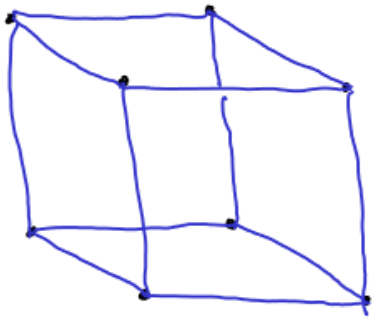
✏ **5.14**
Δείξτε ότι τα δύο γραφήματα του Σχήματος 5.13 δεν είναι ισόμορφα.

✏ **5.15**
Δείξτε ότι δύο γραφήματα είναι ισομορφικά αν και μόνο αν τα συμπληρώματά τους (δείτε Άσκ. 5.1) είναι ισομορφικά.

✏ **5.16**
Βρείτε ένα γράφημα με 5 κορυφές που να είναι ισομορφικό με το συμπληρωματικό του (δείτε Άσκ. 5.1).
5 κορυφές ορίζουν $\binom{5}{2} = 10$ ακμές, άρα το γράφημα αυτό και το συμπληρωματικό του, αφού είναι ισόμορφα, θα έχουνε τον ίδιο αριθμό ακμών, δηλ. 5 ακμές το καθένα.

✏ **5.17**
Θεωρήστε το γράφημα W που έχει ως κορυφές τις ημέρες της εβδομάδας, και όπου δύο μέρες συνδέονται μεταξύ τους με ακμή αν και μόνο αν η μια είναι η επόμενη της άλλης. Επίσης το γράφημα S με σύνολο κορυφών το $\{0, 1, \ldots, 6\}$ όπου δύο κορυφές συνδέονται μεταξύ τους αν και μόνο αν η διαφορά τους mod 7 *ισούται με 3 ή 4 (με άλλα λόγια είναι 3 ή -3* mod 7*). Σχεδιάστε τα δύο γραφήματα και δείξτε ότι είναι ισόμορφα.*

✏ **5.18**
Θεωρήστε το γράφημα Q που έχει ως κορυφές του τις κορυφές ενός τρισδιάστατου κύβου, και το γράφημα B που έχει ως κορυφές όλα τα στοιχεία του συνόλου $\{0, 1\}^3$, όλες δηλ. τις τριάδες από 0 ή 1. Δύο κορυφές του Q συνδέονται αν και μόνο αν συνδέονται με μια ακμή του κύβου. Δύο τριάδες συνδέονται στο B αν και μόνο αν διαφέρουν σε μια ακριβώς συντεταγμένη. Δείξτε ότι τα Q και B είναι ισόμορφα.
Δείτε το Σχήμα 5.15.



Σχήμα 5.15: Το γράφημα της Άσκησης 5.18 που φτιάχνεται από τις κορυφές του κύβου

Το να αποφασίσει κανείς ότι δύο γραφήματα είναι ισόμορφα απαιτεί συνήθως αρκετή δουλειά, μια και, κατ' αρχήν τουλάχιστον, πρέπει να εξετάσει κάθε μια από τις δυνατές συναρτήσεις που απεικονίζουν τις κορυφές του ενός γραφήματος στις κορυφές ενός άλλου και να ελέγξει αν είναι ισομορφισμός. Όμως πολλές φορές μπορεί κανείς να αποφανθεί ότι δύο γραφήματα *δεν* είναι ισόμορφα χρησιμοποιώντας κάποια απλά κριτήρια, όπως αυτά της Άσκησης 5.19.

✏ **5.19**
Έστω G και H δύο απλά γραφήματα. Δείξτε ότι σε κάθε μια από τις παρακάτω περιπτώσεις αυτά δεν είναι ισόμορφα.

1. $|V(G)| \neq |V(H)|$
2. $|E(G)| \neq |E(H)|$
3. *Ο μέγιστος βαθμός κορυφής του G είναι διαφορετικός από το μέγιστο βαθμό κορυφής του H.*
4. *κάθε κορυφή του G συνδέεται με κάθε άλλη με κάποιο μονοπάτι, ενώ υπάρχουν δύο κορυφές του H που δε συνδέονται μεταξύ τους με μονοπάτι.*

Δείξτε επίσης ότι υπάρχουν δύο μη ισόμορφα γραφήματα G και H στα οποία δεν ισχύει κανένα από τα παραπάνω κριτήρια μη ισομορφίας.

Παρατήρηση 5.1
Ένας άλλος τρόπος να περιγράψει κανείς το πότε δύο γραφήματα είναι μεταξύ τους ισόμορφα είναι να κάνει την παρατήρηση ότι είναι ισόμορφα αν και μόνο αν, μπορεί κανείς να πάρει από το ένα το άλλο, απλά με μια μετονομασία των κορυφών τους.

✏ **5.20**
Βρείτε όλα τα μη-ισόμορφα γραφήματα με τέσσερεις κορυφές.

✏ **5.21**
Βεβαιωθείτε ότι τα δύο γραφήματα του Σχ. 6.1 είναι ισόμορφα μεταξύ τους.

5.4 Συνεκτικότητα και αποστάσεις πάνω σε γραφήματα

Ορισμός 5.7
(Μονοπάτι και μήκος του) Μονοπάτι *στο G θα λέγεται μια ακολουθία κορυφών*

$$u_1 \xrightarrow{e_1} u_2 \xrightarrow{e_2} \cdots \xrightarrow{e_{n-1}} u_n,$$

όπου η ακμή e_j συνδέει τις κορυφές u_j και u_{j+1}, $j = 1, \ldots, n-1$. Το πλήθος των ακμών $(n-1)$ που εμφανίζονται σε ένα μονοπάτι θα λέγεται μήκος *του μονοπατιού.*

Ένα μονοπάτι μπορεί να χρησιμοποιεί μια ακμή του γραφήματος παραπάνω από μια φορά.

Παράδειγμα 5.7
Ενα μονοπάτι σε ένα απλό γράφημα μπορούμε να το περιγράψουμε αναφέροντας μόνο τις κορυφές u_j αφού οι ακμές εννοούνται. Π.χ. στο γράφημα του σχήματος 5.2 το $1 \to 2 \to 3 \to 6$ είναι ένα μονοπάτι. Στο γράφημα του Σχήματος 5.1 το Ηράκλειο – Ανώγεια – Ρέθυμνο είναι ένα μονοπάτι μήκους δύο.

✏ **5.22**
Στο γράφημα B της Άσκησης 5.18 βρείτε ένα μονοπάτι που να συνδέει τις κορυφές $(0,0,0)$ και $(1,1,1)$.

Ορισμός 5.8
(Κύκλωμα, κύκλος) **Κύκλωμα** *λέγεται ένα μονοπάτι όπου η τελευταία κορυφή είναι ίδια με την πρώτη.*

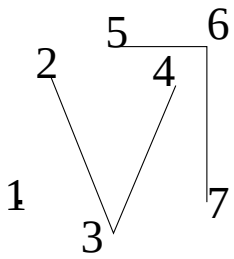
Οταν θέλουμε να μιλήσουμε για κυκλώματα χωρίς επαναλαμβανόμενες ακμές θα τα αποκαλούμε **κύκλους**.

Παράδειγμα 5.8
Στο Σχήμα 5.2 το $1 \to 2 \to 3 \to 6 \to 4 \to 1$ είναι ένα κύκλωμα που είναι ταυτόχρονα και κύκλος αφού καμιά από τις ακμές που συμμετέχουν σε αυτό δεν επαναλαμβάνεται. Στο Σχήμα 5.1 το Ηράκλειο $\to$ Ανώγεια $\to$ Ηράκλειο $\to$ Ρέθυμνο $\to$ Ανώγεια $\to$ Ηράκλειο είναι επίσης ένα κύκλωμα μήκους 5, αλλά όχι κύκλος αφού η ακμή Ηράκλειο – Ανώγεια χρησιμοποιείται 3 φορές.

Ορισμός 5.9
(Προσιτή κορυφή) *Θα λέμε ότι η κορυφή v είναι* **προσιτή** *από την κορυφή u αν υπάρχει μονοπάτι που να ξεκινάει από την u και να καταλήγει στην v.*

Παράδειγμα 5.9
Στα γραφήματα των Σχημάτων 5.1 και 5.2 όλες οι κορυφές είναι προσιτές από όλες.

Είναι εύκολο να δειχτεί ότι η σχέση «v προσιτό από u» είναι μία σχέση ισοδυναμίας πάνω στο σύνολο V των κορυφών. Άρα το σύνολο V διαμερίζεται σε κλάσεις ισοδυναμίας που τις ονομάζουμε *συνεκτικές συνιστώσες*. Με άλλα λόγια δύο κορυφές ενός γραφήματος είναι στην ίδια συνεκτική συνιστώσα αν και μόνο αν υπάρχει μονοπάτι που τις ενώνει.



Σχήμα 5.16: Ενα γράφημα με 3 συνεκτικές συνιστώσες

Παράδειγμα 5.10
Στο σχήμα 5.16 δείχνουμε ένα γράφημα του οποίου οι συνεκτικές συνιστώσες είναι οι $\{1\}$, $\{2,3,4\}$ *και* $\{5,6,7\}$.

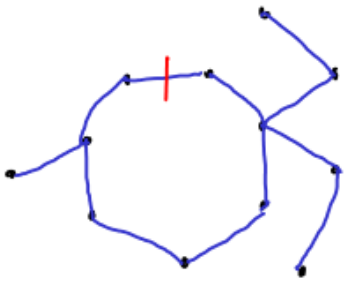
Ορισμός 5.10
(Συνεκτικό γράφημα) *Ενα γράφημα ονομάζεται* **συνεκτικό** *αν έχει μόνο μία συνεκτική συνιστώσα, αν δηλ. κάθε κορυφή συνδέεται με κάθε άλλη μέσω ενός μονοπατιού.*

Παράδειγμα 5.11
Τα γραφήματα των Σχημάτων 5.1 και 5.2 είναι συνεκτικά ενώ αυτό του Σχήματος 5.16 δεν είναι.

✏ **5.23**
Δείξτε ότι ένα συνεκτικό γράφημα με n *κορυφές και λιγότερες από* n *ακμές έχει αναγκαστικά μια κορυφή βαθμού 1.*

💡 *Υποθέστε ότι δεν ισχύει το συμπέρασμα και καταλήξετε σε άτοπο χρησιμοποιώντας την Άσκηση 5.4.*

✏ **5.24**
Δείξτε ότι αν έχουμε ένα συνεκτικό γράφημα που περιέχει ένα κύκλο, και διαγράψουμε μια ακμή αυτού του κύκλου, το γράφημα παραμένει συνεκτικό. Κάτι τέτοιο δε συμβαίνει, εν γένει, αν το γράφημα δεν έχει κύκλο (δώστε παράδειγμα).



Σχήμα 5.17: Συνεκτικό γράφημα με ένα κύκλο του οποίου διαγράφουμε μια ακμή παραμένει συνεκτικό (για Άσκηση 5.24)

Θα ορίσουμε τώρα μια συνάρτηση $d : V \times V \to \mathbb{R}$ που θα έχει την έννοια της **απόστασης**. Η ποσότητα δηλ. $d(u,v)$ θα «μετράει» το πόσο κοντά είναι οι δύο κορυφές u και v του γραφήματος.

Ορισμός 5.11
(Απόσταση κορυφών) *Αν η κορυφή* u *δεν είναι προσιτή από την κορυφή* v *τότε ορίζουμε*

$$d(u,v) = d(v,u) = +\infty,$$

η απόσταση δηλ. ανάμεσα σε δύο κορυφές u *και* v *που δε συνδέονται με κανένα μονοπάτι θεωρείται άπειρη.*

Αλλιώς ορίζουμε $d(u,v)$ *να είναι το ελάχιστο μήκος μονοπατιού που συνδέει τις* u *και* v*, δηλ. του μονοπατιού εκείνου με τις λιγότερες ακμές.*

Παράδειγμα 5.12
Στο Σχήμα 5.16 $d(2,4) = d(5,7) = 2$, $d(3,2) = 1$, *και* $d(1,x) = +\infty$, *για κάθε* $x \in \{2,\dots,7\}$. *Επίσης στο Σχήμα 5.10, αριστερά,* $d(u,v) = 1$, *για κάθε* $u, v \in \{1,\dots,5\}$, $u \neq v$.

Οπως κάθε φυσιολογική έννοια απόστασης στα Μαθηματικά, η συνάρτηση απόστασης που μόλις ορίσαμε ικανοποιεί τη λεγόμενη **τριγωνική ανισότητα**:

$$\forall u, v, w \in V : \quad d(u,v) \leq d(u,w) + d(w,v). \tag{5.2}$$

Για να δεί κανείς γιατί ισχύει αυτό, παρατηρήστε ότι αν πάρουμε οποιοδήποτε μονοπάτι από το u στο w και το συνεχίσουμε με ένα οποιοδήποτε μονοπάτι από το w στο v, τότε παίρνουμε ένα μονοπάτι από το u στο v. Οι λεπτομέρειες της απόδειξης αφήνονται στον αναγνώστη.

✏ **5.25**
Αποδείξτε την (5.2) *με όλες τις λεπτομέρειες.*

Εχοντας ορίσει μια έννοια απόστασης, μπορούμε τώρα να μιλήσουμε για τη *διάμετρο* ενός γραφήματος $G = (V, E)$, που τη συμβολίζουμε με $\operatorname{diam} G$.

Ορισμός 5.12
(Διάμετρος) *Η διάμετρος ενός γραφήματος* G *ορίζεται να είναι η μέγιστη απόσταση ανάμεσα σε δυό κορυφές του* G*:*

$$\operatorname{diam} G = \max_{u,v \in V} d(u,v). \tag{5.3}$$

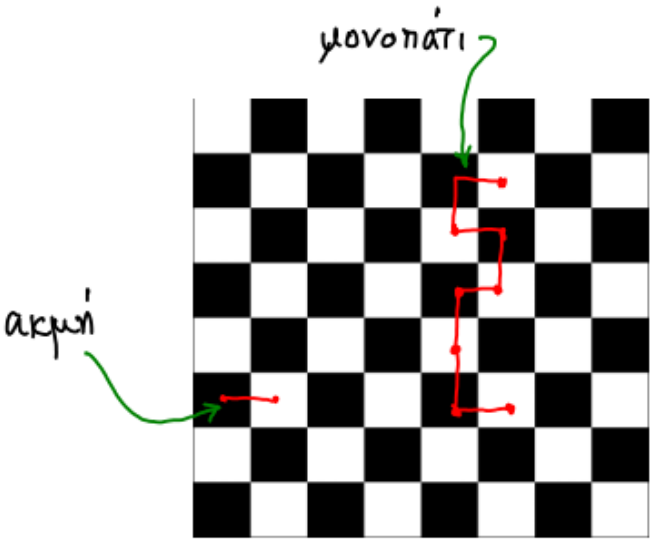
Είναι φανερό ότι ένα γράφημα G είναι συνεκτικό αν και μόνο αν $\operatorname{diam} G < \infty$. Για παράδειγμα, το αριστερό γράφημα του Σχήματος 4 έχει διάμετρο 1 ενώ το δεξιό έχει διάμετρο 2.

✏ **5.26**
Ποια η διάμετρος του γραφήματος B *της Άσκησης 5.18;*

✏ **5.27**
Δείξτε ότι η διάμετρος ενός συνεκτικού γραφήματος με n *κορυφές είναι το πολύ* $n - 1$.
Περιγράψτε, με πλήρη απόδειξη, όλα τα γραφήματα με n *κορυφές και διάμετρο* $n - 1$.
Επίσης όλα τα γραφήματα με διάμετρο $n - 2$ *και όλα τα γραφήματα με διάμετρο 1.*
💡 *Για το πρώτο παρατηρήστε ότι αν* u, v *είναι δυο κορυφές του* G *με απόσταση* $d = d(u,v)$ *τότε υπάρχει ένα μονοπάτι που τις ενώνει χωρίς επαναλαμβανόμενες ακμές. Κάθε μονοπάτι που τις ενώνει και έχει μήκος* d *είναι τέτοιο (αλλιώς η απόστασή τους θα ήταν μικρότερη).*

✏ **5.28**
Όλοι οι κάτοικοι μιας χώρας, της οποίας το αλφάβητο έχει 10 γράμματα, έχουν ως όνομα μια λέξη μήκους ακριβώς 6. Το πλήθος των κατοίκων είναι 10^6 *και όλοι έχουν διαφορετικά ονόματα. Αν* G *είναι το γράφημα με κορυφές τους κατοίκους, και δύο κάτοικοι συνδέονται με ακμή αν και μόνο αν τα ονόματά τους διαφέρουν σε ακριβώς μια θέση, ποια είναι η διάμετρος του* G*;*
💡 *Δύο κάτοικοι συνδέονται μεταξύ τους με ακμή αν και μόνο αν μπορούμε να αλλάξουμε το όνομα του ενός σε ακριβώς μια θέση και να πάρουμε το όνομα του άλλου. Σκεφτόμενοι έτσι βλέπουμε ότι το να διασχίσουμε μια ακμή στο γράφημα ισοδυναμεί με το να αλλάξουμε το όνομα της τρέχουσας κορυφής σε μια ακριβώς θέση. Άρα το ερώτημα «ποια είναι η διάμετρος του* G*» ισοδυναμεί με το ερώτημα «πόσες το πολύ αλλαγές πρέπει να κάνουμε στο όνομα ενός κατοίκου για να πάρουμε το όνομα ενός άλλου κατοίκου;»*

✏ **5.29**
Ένα γράφημα έχει ως κορυφές τα 64 τετραγωνάκια μιας συνηθισμένης σκακιέρας, και δύο τετραγωνάκια συνδέονται μεταξύ τους με ακμή αν και μόνο αν έχουν μια πλευρά κοινή. Ποια η διάμετρος του γραφήματος;



Σχήμα 5.18: Το γράφημα της Άσκησης 5.29.

✏ **5.30**

Δείξτε ότι σε κάθε συνεκτικό γράφημα υπάρχει μια κορυφή τέτοια ώστε αν διαγράψουμε αυτή την κορυφή και τις ακμές που καταλήγουν σε αυτή το επαγόμενο γράφημα παραμένει συνεκτικό.

💡 *Ας είναι a, b δύο κορυφές του γραφήματος G με $d(a,b) = \operatorname{diam} G$. Δείξτε ότι κάθε μια από τις a, b μπορεί να παίξει το ρόλο της προς διαγραφή κορυφής της Άσκησης.*

✏ **5.31**

Αν σε ένα γράφημα υπάρχουν ακριβώς δύο κορυφές με περιττό βαθμό, αυτές πρέπει αναγκαστικά να συνδέονται με κάποιο μονοπάτι.

💡 *Δείτε την Άσκηση 5.6.*

✏ **5.32**

Ο απλούστερος ίσως τρόπος, αν και όχι πάντα ο πιο αποτελεσματικός από άποψη υπολογιστική, για να παραστήσει κανείς ένα απλό γράφημα είναι με το λεγόμενο **πίνακα συνδεσμολογίας**. *Εστω $G = (V, E)$ ένα απλό γράφημα με $V = \{v_1, \ldots, v_n\}$. Ο πίνακας συνδεσμολογίας A είναι τότε ένας $n \times n$ πίνακας με*

$$A_{ij} = \begin{cases} 1 & \alpha\nu\ v_i \sim v_j, \\ 0 & \alpha\lambda\lambda\iota\omega\varsigma. \end{cases}$$

Βάζουμε δηλ. 1 στη θέση i, j αν και μόνο αν η i-οστή και η j-οστή κορυφή συνδέονται με κάποια ακμή. Από τον ορισμό προκύπτει αμέσως ότι ο πίνακας A είναι συμμετρικός και έχει 0 παντού πάνω στη διαγώνιο. (Θυμίζουμε ότι μιλάμε εδώ για **απλά γραφήματα**, *γραφήματα δηλ. στα οποία οι ακμές δεν έχουν κατεύθυνση και καμιά κορυφή δε συνδέεται με τον εαυτό της. Όταν αυτές οι ιδιότητες δεν ισχύουν τότε μπορεί και ο πίνακας συνδεσμολογίας είτε να μην είναι συμμετρικός είτε να μην έχει μόνο μηδενικά στη διαγώνιο.)*

*Με επαγωγή ως προς k δείξετε ότι Ο πίνακας A^k, $k \geq 0$, (γινόμενο του πίνακα A με τον εαυτό του k φορές) έχει στη θέση i, j τον αριθμό s αν και μόνο αν ο αριθμός των μονοπατιών μήκους k από την κορυφή i στην j είναι ακριβώς s. (*Παρατήρηση: *Ενα μονοπάτι μήκους k από το u στο v μπορεί να επαναλαμβάνει ακμές. Για παράδειγμα, αν $u \sim u_1 \sim v$, τότε το μονοπάτι $u \to u_1 \to u \to u_1 \to v$ είναι ένα μονοπάτι από το u στο v μήκους 4.)*

💡 *Αν X, Y είναι $n \times n$ πίνακες και $Z = XY$ είναι το γινόμενό τους (επίσης $n \times n$ πίνακας) τότε εξ ορισμού*

$$Z_{i,j} = \sum_{r=1}^{n} X_{i,r} Y_{r,j}, \quad \gamma\iota\alpha\ i, j = 1, 2, \ldots, n.$$

Ισχύει λοιπόν

$$A^k_{i,j} = \sum_{r=1}^{n} A^{k-1}_{i,r} A_{r,j}, \ \ \gamma\iota\alpha\ i,j = 1,2,\ldots,n. \tag{5.4}$$

Με βάση την επαγωγική υπόθεση η ποσότητα $A^{k-1}_{i,r}$ μας δίνει το πλήθος των μονοπατιών από την κορυφή i στην κορυφή r με μήκος ακριβώς $k-1$. Χρησιμοποιώντας αυτό ερμηνεύστε το άθροισμα της (5.4) ως το πλήθος των μονοπατιών από την κορυφή i στην κορυφή j με μήκος ακριβώς k.

✏ **5.33**
Αν G είναι ένα συνεκτικό γράφημα με n κορυφές, μέγιστο βαθμό d τότε

$$n \leq 1 + d\frac{(d-1)^{\operatorname{diam} G} - 1}{d-2}.$$

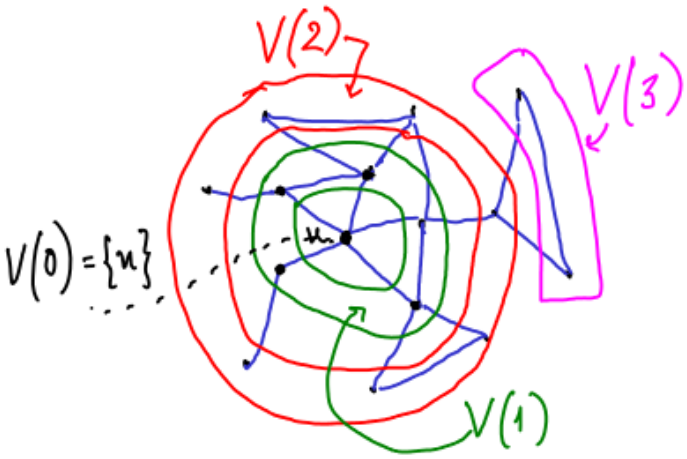
Έστω u μια κορυφή του G. Τα σύνολα κορυφών

$$V(k) = \{v \in V :\ d(u,v) = k\}, \ \ k = 0,1,\ldots,\operatorname{diam} G,$$

διαμερίζουν το σύνολο κορυφών V. Δείξτε με επαγωγή ως προς k ότι

$$|V(k)| \leq d(d-1)^{k-1} \ \ \gamma\iota\alpha\ k \geq 1.$$

Αθροίστε έπειτα αυτές τις ανισότητες για $k = 0,1,\ldots,\operatorname{diam} G$ και χρησιμοποιήστε τον τύπο για την πεπερασμένη γεωμετρική σειρά (1.15).

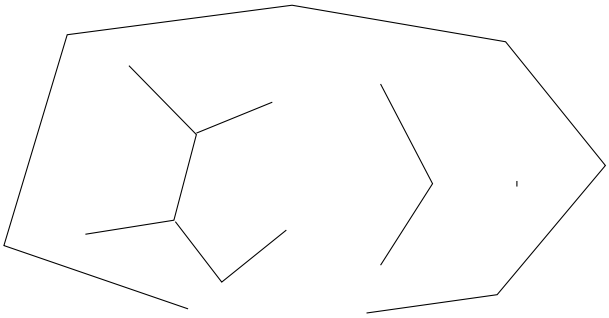


Σχήμα 5.19: Τα σύνολα $V(0), V(1), V(2), V(3)$ της υπόδειξης της Άσκησης 5.33 σε ένα παράδειγμα. Το σύνολο $V(1)$ είναι οι κορυφές που απέχουν απόσταση 1 από το u (πράσινος «δακτύλιος»), το σύνολο $V(2)$ είναι οι κορυφές που απέχουν απόσταση 2 από το u (κόκκινος «δακτύλιος»), και το σύνολο $V(3)$ είναι οι κορυφές που απέχουν απόσταση 3 από το u (μώβ περιοχή).

5.5 Δέντρα και δάση

Τα δέντρα είναι, κατά κάποιο τρόπο, τα συνεκτικά γραφήματα χωρίς περιττές ακμές.

Ορισμός 5.13
(Δέντρα, δάση) *Ενα συνεκτικό γράφημα που δεν περιέχει κύκλους ονομάζεται* δέντρο. *Ενα γράφημα, συνεκτικό ή μη, που δεν περιέχει κύκλους ονομάζεται* δάσος.



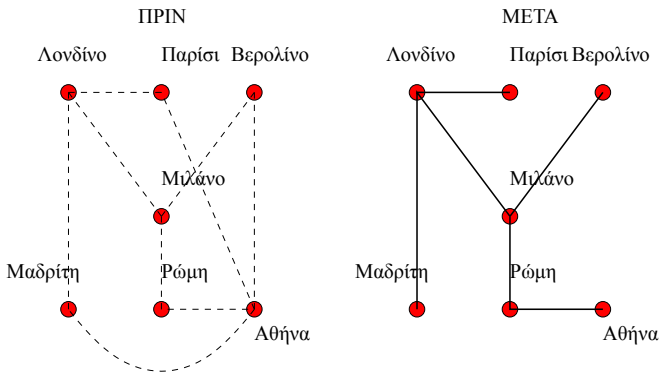
Σχήμα 5.20: Ένα δάσος από 4 δέντρα

Η δεύτερη ονομασία είναι συμβατή με την πρώτη αφού κάθε τέτοιο γράφημα μπορεί να το δει κανείς σαν το σύνολο των συνεκτικών συνιστωσών του. Αλλά κάθε τέτοια συνεκτική συνιστώσα εξακολουθεί να μην περιέχει κύκλους (αφού είναι υπογράφημα του αρχικού), άρα είναι ένα δέντρο, δηλ. κάθε γράφημα χωρίς κύκλους είναι μια «ξένη» (δηλ. χωρίς μεταξύ τους συνδέσεις) ένωση από δέντρα. Με άλλα λόγια, ένα γράφημα είναι δάσος αν και μόνο είναι μια ένωση από, ασύνδετα μεταξύ τους, δέντρα.

Τα δέντρα έχουν ενδιαφέρον επειδή, κατά κάποια έννοια, είναι τα «ελάχιστα» συνεκτικά γραφήματα: κάθε συνεκτικό γράφημα $G = (V, E)$ περιέχει ένα υπογράφημα με τις ίδιες κορυφές, συνεκτικό και χωρίς κύκλους (άρα δέντρο). (Δείτε το Θεώρημα 5.1.)

Παράδειγμα 5.13

Ας πούμε ότι έχουμε ένα γράφημα (Σχήμα 5.21) με τα δρομολόγια που εκτελεί μια αεροπορική εταιρεία ανάμεσα σε N πόλεις. Κάποιες πόλεις συνδέονται μεταξύ τους απ' ευθείας, κάποιες με μία ενδιάμεση στάση, κ.λ.π.



Σχήμα 5.21: Τα δρομολόγια μιας αεροπορικής εταιρείας, πριν και μετά τις περικοπές

Σε κάποια άσχημη οικονομική συγκυρία η εταιρεία αποφασίζει πως δεν είναι πλέον σε θέση να εκτελεί τόσο πολλά δρομολόγια και ότι πρέπει να καταργήσει όσο πιο πολλά μπορεί. Η εταιρεία δε θα εισαγάγει νέα δρομολόγια, απλώς θα καταργήσει μερικά. Για λόγους πολιτικής όμως η εταιρεία δε μπορεί να σταματήσει να εξυπηρετεί καμία από τις N πόλεις που μέχρι τότε εξυπηρετούσε. Επίσης, προσεγγιστικά, όλες οι πτήσεις κοστίζουν το ίδιο στην εταιρεία, ανεξάρτητα από την απόσταση.

Δείχνουμε στο Σχήμα 5.21 τη λύση που επέλεξε τελικά η εταιρεία. Παρατηρήστε ότι:

- *Για τις 7 πόλεις χρησιμοποιούνται πλέον 6 πτήσεις (ακμές στο γράφημα).*
- *Για κάθε ζεύγος πόλεων εξακολουθεί να είναι δυνατό να πάει κανείς από τη μια στην άλλη, με κατάλληλες ενδιάμεσες στάσεις, και*

- *Για κάθε ζεύγος πόλεων υπάρχει μόνο ένας τρόπος να ταξιδέψει κανείς από τη μια στην άλλη (χωρίς, εννοείται, να πετάει μπρος πίσω).*

Ορισμός 5.14
(Δέντρα και δάση που παράγουν) *Ενα δέντρο T, υπογράφημα του G και με τις ίδιες κορυφές, λέγεται* δέντρο που παράγει το G *(spanning tree). Αν το T δεν είναι δέντρο αλλά είναι δάσος, και κάθε συνεκτική συνιστώσα του G παράγεται από κάποιο δέντρο του T, τότε το T λέγεται* δάσος που παράγει το G.

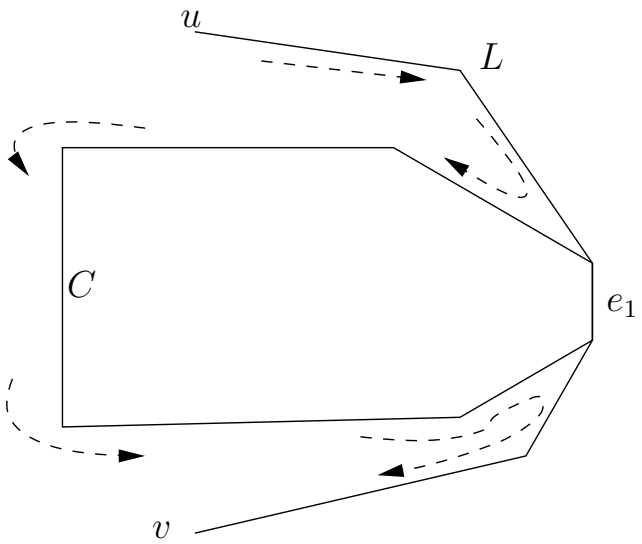
Θεώρημα 5.1
Κάθε συνεκτικό γράφημα G περιέχει ένα δέντρο που το παράγει.

Απόδειξη

Εστω ότι το συνεκτικό γράφημα $G = (V, E)$ περιέχει κάποιο κύκλο

$$C : u_1 \xrightarrow{e_1} u_2 \xrightarrow{e_2} \cdots \xrightarrow{e_{n-1}} u_n = u_1.$$

Ας επιλέξουμε τυχαία μια από τις ακμές του κύκλου, π.χ. την e_1, και ας τη σβήσουμε από το γράφημα. Ισχυριζόμαστε ότι το γράφημα παραμένει συνεκτικό. (Δείτε και την Άσκηση 5.24.) Πραγματικά, ας υποθέσουμε πως η ακμή e_1 που σβήσαμε συμμετείχε στο γράφημα G σε κάποιο μονοπάτι L που συνέδεε δύο κορυφές v και u, όπως φαίνεται στο Σχ. 5.22.



Σχήμα 5.22: Διαγραφή της e_1 διατηρεί τη συνεκτικότητα

Είναι φανερό ότι, παρά το ότι τώρα πια η ακμή e_1 έχει διαγραφεί, μπορούμε και πάλι να πάμε από το v στο u διανύοντας το μονοπάτι όπως και πριν αλλά όταν θα χρειαστεί να περάσουμε την e_1 μπορούμε να την αντικαταστήσουμε διανύοντας το υπόλοιπο του κύκλου C.

Την πράξη αυτή, που μόλις δείξαμε ότι διατηρεί τη συνεκτικότητα, την ονομάζουμε «σπάσιμου του κύκλου C στην ακμή e_1». Επαναλαμβάνοντας αυτή την πράξη όσο εξακολουθούν να υπάρχουν κύκλοι στο γράφημα, και αφού μετά από κάθε τέτοια πράξη οι ακμές λιγοστεύουν κατά μία, είναι φανερό (εφόσον μιλάμε για πεπερασμένα γραφήματα) ότι θα φτάσουμε σε ένα υπογράφημα του G με τις ίδιες κορυφές (αυτές δεν αλλάζουν με την πράξη της διαγραφής της ακμής), συνεκτικό και χωρίς πλέον κύκλους, δηλ. σε ένα δέντρο.

Αν το γράφημα G δεν είναι συνεκτικό εφαρμόζουμε το πρώτο κομμάτι (που μόλις αποδείξαμε) του Θεωρήματος 5.1 σε κάθε συνεκτική του συνιστώσα και παίρνουμε έτσι από ένα δένδρο για κάθε συνιστώσα, που την παράγει.

■

Το επόμενο θεώρημα μας λέει ότι, αντίθετα με τα γενικά γραφήματα, το πλήθος των ακμών σε ένα δέντρο είναι πλήρως καθορισμένο από το πλήθος των κορυφών του.

Θεώρημα 5.2
Κάθε δέντρο με n κορυφές έχει ακριβώς $n-1$ ακμές.

Απόδειξη

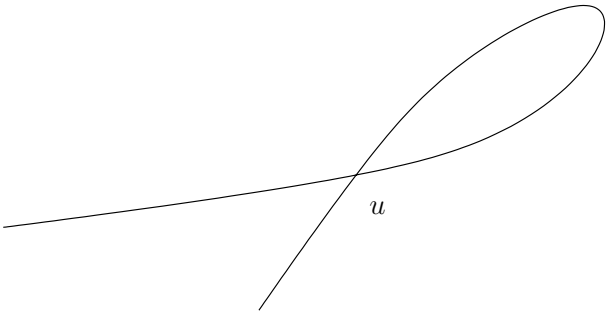
Με επαγωγή ως πρός n. Για $n = 1$ είναι προφανές. Εστω G δέντρο με n κορυφές.

Ισχυρισμός: Υπάρχει κορυφή του G με βαθμό 1.

Εστω ότι όλες οι κορυφές έχουν βαθμό ≥ 2 (αφού καμία δεν έχει βαθμό 0 λόγω συνεκτικότητας). Μπορούμε τότε να βρούμε μονοπάτια οσουδήποτε μεγάλου μήκους στο G στα οποία ποτέ δεν εμφανίζεται κάτι της μορφής

$$\cdots u \xrightarrow{e} v \xrightarrow{e} u \cdots$$

αφού πάντα μπορούμε να φύγουμε από κάποια κορυφή χρησιμοποιώντας κάποια άλλη ακμή από αυτή που χρησιμοποιήσαμε για να μπούμε, και μπορούμε να κινούμαστε έτσι επ' άπειρον. Αν το μονοπάτι έχει αρκετά μεγάλο μήκος θα υπάρχει σίγουρα κάποια κορυφή που εμφανίζεται εκεί πάνω από μία φορά. Επιλέγουμε μια τέτοια κορυφή u που έχει επιπλέον την ιδιότητα ότι η απόσταση ανάμεσα στις δύο εμφανίσεις της είναι ελάχιστη.



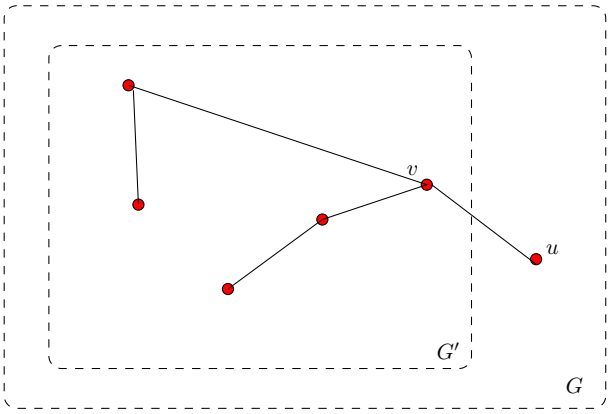
Σχήμα 5.23: Ενα μονοπάτι με μια επαναλαμβανόμενη κορυφή u

Η κατάσταση απεικονίζεται στο Σχήμα 5.23. Η επιπλέον ιδιότητα αυτή της u συνεπάγεται ότι στο κύκλωμα που απεικονίζεται στο σχήμα πάνω από το u δεν υπάρχει άλλη επαναλαμβανόμενη κορυφή ή ακμή, άρα αυτό το κύκλωμα είναι κύκλος, πράγμα που απαγορεύεται σε δέντρο, και έχουμε αποδείξει τον ισχυρισμό. (Δείτε και την Άσκηση 5.23.)

Εστω λοιπόν $\deg u = 1$ και ορίζουμε το υπογράφημα G' του G που επάγεται από τις υπόλοιπες κορυφές $V \setminus \{u\}$, σβήνουμε δηλ. την u και τη μοναδική ακμή που καταλήγει στην u. (Δείτε Σχήμα 5.24.)

Ως υπογράφημα, το G' προφανώς δεν έχει κύκλους και εξακολουθεί να είναι συνεκτικό αφού είναι φανερό ότι, επειδή η u έχει βαθμό 1, δεν μπορεί να χρησιμοποιθεί για τη σύνδεση δύο άλλων κορυφών. Αλλά το G' έχει $n-1$ κορυφές και από την επαγωγική μας υπόθεση έχει συνεπώς $n-2$ ακμές. Αρα το G έχει $n-1$ (αυτές του G' συν αυτή που καταλήγει στην u).
■

✏ **5.34**
Αποδείξτε ότι ένα δάσος με n κορυφές και m συνεκτικές συνιστώσες (m δέντρα δηλαδή) έχει ακριβώς $n-m$ ακμές.
Εφαρμόστε το Θεώρημα 5.2 σε κάθε δέντρο του δάσους (δηλ. σε κάθε συνεκτική συνιστώσα του γραφήματος).



Σχήμα 5.24: Σβήνουμε την κορυφή u και τη μοναδική ακμή που καταλήγει σε αυτή για να πάρουμε το υπογράφημα G' από το G.

✏ **5.35**

Δείξτε ότι κάθε ζεύγος κορυφών ενός δέντρου ενώνονται μεταξύ τους με ένα μοναδικό μονοπάτι το οποίο δεν περνά δύο φορές από την ίδια ακμή. Δείξτε επίσης ότι αν ισχύει αυτό για ένα γράφημα G τότε αυτό είναι αναγκαστικά δέντρο.

Σε κάθε συνεκτικό γράφημα και για κάθε δύο κορυφές του υπάρχει μονοπάτι μεταξύ τους χωρίς επαναλαμβανόμενες ακμές (π.χ. κάθε μονοπάτι που τις ενώνει και είναι ελάχιστου μήκους). Θα πρέπει να δείξετε ότι αν το γράφημα είναι δέντρο τότε αυτό το μονοπάτι είναι μοναδικό. Επίσης, για το αντίστροφο, ότι αν σε κάποιο συνεκτικό γράφημα ισχύει η μοναδικότητα για κάθε ζεύγος κορυφών του *τότε αυτό είναι δέντρο.*

Για να δείξετε τη μοναδικότητα (στην περίπτωση που το γράφημα είναι δέντρο) υποθέστε, αντίθετα με αυτό που θέλετε να αποδείξετε, ότι οι κορυφές u, v του δέντρου G συνδέονται με δύο διαφορετικά μονοπάτια π_1, π_2 μεταξύ τους. Κάθε ένα από τα π_1, π_2 δεν περιέχει επαναλαμβανόμενες ακμές.

Η εύκολη περίπτωση είναι όταν καμιά ακμή του π_1 δεν υπάρχει στο π_2. Σε αυτή την περίπτωση το κύκλωμα που δημιουργείται αρχίζοντας από την κορυφή u, ακολουθώντας το π_1 ως την κορυφή v, και απιστρέφοντας στην κορυφή u ακολουθώντας το p_2 ανάποδα, δεν είναι απλά ένα κύκλωμα αλλά κύκλος, *δεν περιέχει δηλ. επαναλαμβανόμενες ακμές. Αυτό αντιφάσκει με το ότι το γράφημα μας είναι δέντρο (=συνεκτικό και χωρίς κύκλους).*

Γενικά μπορεί όμως μια ακμή του π_1 να υπάρχει και στο π_2 οπότε ο κύκλος που θα πρέπει να βρούμε για να έχουμε αντίφαση δε μπορεί να είναι η προηγούμενος και χρειάζεται κάπως προσεκτική δουλειά.

✏ **5.36**

Δείξτε ότι αν προσθέσουμε μια ακμή σε ένα δέντρο τότε δημιουργούμε ακριβώς ένα κύκλο.

Αν το δέντρο μας έχει n κορυφές τότε έχει ακριβώς $n-1$ ακμές. Μετά την πρόσθεση μιας ακμής θα έχει n ακμές και παραμένει φυσικά συνεκτικό, άρα δεν παραμένει δέντρο και το νέο μας γράφημα θα περιέχει κάποιο κύκλο. Θα πρέπει να δείξετε ότι περιέχει μόνο ένα κύκλο.

Εύκολα έχουμε τώρα:

Πόρισμα 5.1
Αν ένα συνεκτικό γράφημα G με n κορυφές έχει $n-1$ ακμές τότε είναι δέντρο.

Απόδειξη

Το G περιέχει κάποιο δέντρο που παράγει, έστω T, το οποίο έχει $n-1$ ακμές σύμφωνα με το Θεώρημα 5.2. Αρα $G = T$.

■

✏ **5.37**
Ένα συνεκτικό γράφημα με τουλάχιστον 3 κορυφές λέγεται **διπλά συνεκτικό** *αν παραμένει συνεκτικό ακόμη κι αν σβήσουμε μια οποιαδήποτε ακμή του. Πόσες, το λιγότερο, ακμές πρέπει να έχει ένα τέτοιο γράφημα με n κορυφές; Βρείτε ένα γράφημα που να «πιάνει» τον ελάχιστο αυτό αριθμό ακμών.*
Πόρισμα 5.1.

✏ **5.38**
Έστω συνεκτικό γράφημα G με τουλάχιστον 3 κορυφές. Μια ακμή του, την οποία αν αφαιρέσουμε αποσυνδέουμε το γράφημα, λέγεται **γέφυρα**. *Δηλ. ένα συνεκτικό γράφημα είναι διπλά συνεκτικό (δείτε Άσκηση 5.37) αν και μόνο αν δεν έχει γέφυρες.*
(α) Δείξτε ότι μια ακμή είναι γέφυρα αν και μόνο αν δεν περιέχεται σε κανένα κύκλο.
(β) Δείξτε ότι κάθε ακμή του G είναι γέφυρα αν και μόνο αν το G είναι δέντρο.

5.6 Γενικεύσεις της έννοιας του γραφήματος

Ορισμός 5.15
(Κατευθυνόμενα γραφήματα) Κατευθυνόμενα γραφήματα *είναι ζευγάρια (V, E), όπου και πάλι V είναι ένα σύνολο κορυφών, αλλά το σύνολο E των ακμών είναι τώρα όχι ένα σύνολο διμελών υποσυνόλων του V αλλά ένα σύνολο διατεταγμένων ζευγών με στοιχεία από το V, δηλ. $E \subseteq V \times V$.*

Ανάλογα με την περίπτωση μπορεί κανείς να επιτρέπει ή όχι και ζευγάρια της μορφής (v, v) (τέτοιες ακμές ονομάζονται *βρόχοι*). Το σημαντικό πάντως είναι ότι δε μπορεί πλέον κανείς να λέει ότι «i συνδέεται με το j» αλλά πρέπει να προσδιορίζει και την κατεύθυνση της σύνδεσης.

Ορισμός 5.16
(Πολλαπλές ακμές) *Γραφήματα με πολλαπλές ακμές είναι αυτά (κατευθυνόμενα ή μη) στα οποία μια ακμή μπορεί να μην υπάρχει καθόλου, να υπάρχει μια φορά, δυο φορές, κλπ. Ο αριθμός των φορών που εμφανίζεται μια ακμή λέγεται* **πολλαπλότητα** *της ακμής.*

Ορισμός 5.17
(Αυτοσυνδέσεις ή βρόχοι) Γραφήματα με αυτοσυνδέσεις *(κατευθυνόμενα ή μη) είναι αυτά στα οποία επιτρέπουμε μια κορυφή να συνδέεται με τον εαυτό της. Μια τέτοια ακμή ονομάζεται αυτοσύνδεση ή βρόχος.*

Ορισμός 5.18
(Βάρη στις ακμές) Γραφήματα με βάρη/κόστη *είναι αυτά (κατευθυνόμενα ή μη) στα οποία κάθε ακμή έχει και ένα βάρος/κόστος.*

Αυτά τα βάρη είναι συνήθως μη αρνητικοί αριθμοί, αλλά αυτό δεν είναι απαραίτητο και εξαρτάται από την εφαρμογή. Για παράδειγμα, αν οι κορυφές παριστάνουν πόλεις σε μία χώρα και οι ακμές κάποιους δρόμους που τις συνδέουν, τα βάρη μπορούν να παριστάνουν τα μήκη των δρόμων.

Στο Σχήμα 5.25 δείχνουμε δύο γραφήματα. Το αριστερό είναι ένα κατευθυνόμενο γράφημα με σύνολα κορυφών και ακμών τα

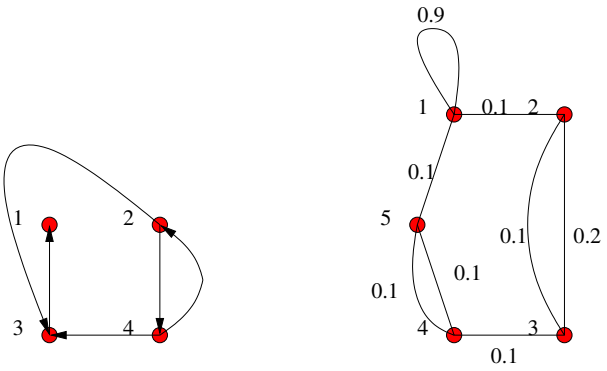
$$V = \{1, 2, 3, 4\}$$

$$E = \{(2, 3), (2, 4), (3, 1), (4, 2), (4, 3)\}$$

και το δεξί είναι ένα γράφημα με πολλαπλές ακμές, με αυτοσυνδέσεις και βάρη πάνω στις ακμές. Είναι φανερό ότι μπορούν να υπάρξουν διάφοροι τέτοιοι συνδυασμοί.

Η έννοια του μονοπατιού σε μη απλά γραφήματα είναι σχεδόν ταυτόσημη με αυτή που ισχύει στα απλά γραφήματα, αν όμως το γράφημα είναι κατευθυνόμενο τότε φυσιολογικά απαιτούμε οι ακμές να έχουν όλες φορά από μια κορυφή του μονοπατιού προς την επόμενη.

Ειδικά για τα γραφήματα με μη αρνητικά βάρη υπάρχει μια επιπλέον έννοια της απόστασης ανάμεσα σε δύο κορυφές που λαμβάνει υπόψην της τα «μήκη» (ή βάρη) των ακμών.

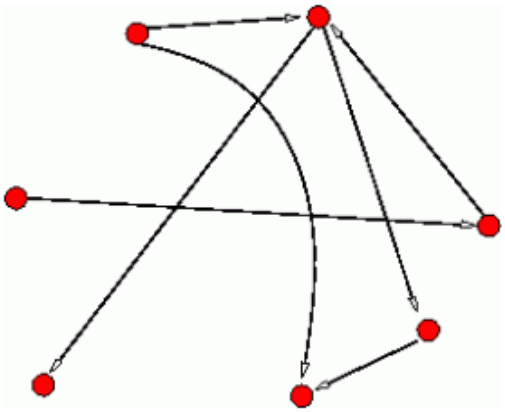


Σχήμα 5.25: Μη απλά γραφήματα

Ορισμός 5.19
(Απόσταση σε γραφήματα με βάρη) *Ετσι, το* **μήκος** *ενός μονοπατιού σε ένα γράφημα με βάρη είναι απλώς το άθροισμα των βαρών των ακμών που συμμετέχουν στο μονοπάτι. Η* **απόσταση** *ανάμεσα στις κορυφές u και v ορίζεται ως το ελάχιστο μήκος μονοπατιού που συνδέει τις u και v ($+\infty$ αν δεν συνδέονται με κάποιο μονοπάτι), και η* **διάμετρος** *του γραφήματος G ορίζεται ως η μέγιστη απόσταση ανάμεσα σε δύο κορυφές του G, όπως και πριν.*

✏ **5.39**
Δείξτε ότι η τριγωνική ανισότητα (5.2) εξακολουθεί να ισχύει και για τη νέα έννοια απόστασης (πάντα μιλάμε για γραφήματα με μη αρνητικά βάρη).

Η απόδειξη είναι σχεδόν ταυτόσημη με αυτή για τη συνηθισμένη έννοι απόστασης σε απλά γραφήματα.



Σχήμα 5.26: Για την Άσκηση 5.40

✏ **5.40**
Σε μια χώρα υπάρχουν N πόλεις και ακριβώς N δρόμοι ανάμεσά τους, όλοι μονόδρομοι, όπως φαίνεται στο Σχήμα 5.26. Φυσικά κάποιες πόλεις μπορεί και να μην έχουν καθόλου δρόμους που να ξεκινάνε ή να καταλήγουν σε αυτές.

Ας ονομάσουμε Z τον αριθμό των πόλεων στις οποίες δεν καταλήγει κανείς δρόμος και E τον αριθμό των πόλεων στις οποίες καταλήγει άρτιος αριθμός δρόμων (του 0 συμπεριλαμβανομένου). Στο Σχήμα 5.26 έχουμε $Z = 2$ και $E = 4$.

Δείξτε ότι $2Z \geq E$.

5.7 Ο αλγόριθμος του Kruskal για ελάχιστα δέντρα που παράγουν σε γραφήματα με βάρη

Εστω $G = (V, E)$ ένα συνεκτικό γράφημα με μη αρνητικά βάρη στις ακμές του

$$w : E \to \mathbb{R}^+.$$

Μας ενδιαφέρει να επιλέξουμε εκείνο το δέντρο T από όλα τα δυνατά δέντρα που παράγουν το G που το βάρος του, δηλ. το άθροισμα των ακμών που συμμετέχουν στο δέντρο, να είναι όσο γίνεται πιο μικρό. Θέλουμε δηλ. να ελαχιστοποιήσουμε την ποσότητα

$$w(T) = \sum_{e \in T} w(e),$$

όπου το άθροισμα παίρνεται πάνω απ'όλες τις ακμές e που εμφανίζονται στο δέντρο ($e \in T$), και το T είναι ένα δέντρο που παράγει το G, έχει δηλ. το ίδιο σύνολο κορυφών με το γράφημα G.

Ορισμός 5.20
(Ελάχιστο δέντρο που παράγει) *Αν και η ποσότητα $w(T)$ έχει μοναδικό ελάχιστο, αυτό μπορεί να «πιάνεται» για παραπάνω από ένα δέντρα που παράγουν. Ολα αυτά τα δέντρα με ελάχιστο βάρος τα ονομάζουμε* ελάχιστα δέντρα *του G.*

Μπορεί κανείς σχετικά εύκολα να δείξει ότι ο παρακάτω αλγόριθμος όντως βρίσκει ένα ελάχιστο δέντρο που παράγει στο G.
Ο αλγόριθμος του Kruskal

1. Δημιουργούμε ένα δάσος F από δέντρα όπου κάθε κορυφή του G αποτελεί και ένα δέντρο.
2. Δημιουργούμε ένα σύνολο S που περιέχει όλες τις ακμές του G, διατεταγμένες σε αύξουσα σειρά βάρους.
3. Όσο ισχύει $S \neq \emptyset$ επαναλαμβάνουμε τα παρακάτω:
   (α) Αφαιρούμε την πρώτη ακμή του S (που είναι μια από αυτές που έχουν το ελάχιστο βάρος ανάμεσα στις ακμές που περιέχονται στο S).
   (β) Αν αυτή η ακμή ενώνει μεταξύ τους δύο διαφορετικά δέντρα του δάσους F, τότε προσθέτουμε αυτή την ακμή στο F, ενώνοντας έτσι σε ένα δύο δέντρα του F. Αλλιώς την πετάμε αυτή την ακμή.

Αποδεικνύεται ότι στο τέλος του αλγορίθμου το δάσος F περιέχει μόνο ένα δέντρο που είναι ένα ελάχιστο δέντρο του G. (Με τις κατάλληλες δομές δεδομένων ο αλγόριθμος του Kruskal χρειάζεται χρόνο $O(m \log m)$ για να τελειώσει, όπου m είναι το πόσες ακμές έχει το γράφημα G.)

Θεώρημα 5.3
Ο αλγόριθμος του Kruskal που περιγράψαμε προηγουμένως όντως βρίσκει ένα ελάχιστο δέντρο για το γράφημα G.

Απόδειξη

Το ότι το γράφημα που παράγεται από τον αλγόριθμο του Kruskal είναι ανά πάσα χρονική στιγμή ένα δάσος είναι φανερό, αφού κάθε τέτοιο γράφημα προκύπτει από το προηγούμενο με την προσθήκη μιας ακμής η οποία ενώνει δύο διαφορετικά δέντρα του προηγουμένου, και επειδή είναι φανερό ότι αν ενώσουμε με μια ακμή δύο δέντρα με διαφορετικό σύνολο κορυφών παίρνουμε πάλι ένα δέντρο.

Επίσης το δάσος F είναι, στο τέλος του αλγορίθμου, ένα και μόνο δέντρο. Αλλιώς το F θα περιείχε τις συνεκτικές συνιστώσες $C_1, \ldots, C_k$, $k > 1$, και, από τον τρόπο που δουλεύει ο αλγόριθμος, αυτό

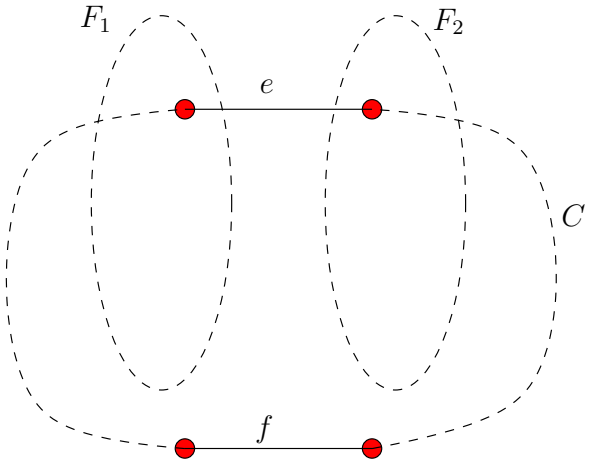
συνεπάγεται ότι καμιά από τις ακμές του G δεν ενώνει μεταξύ τους δύο διαφορετικά C_j. Αυτό σημαίνει όμως ότι το G δεν είναι συνεκτικό, άτοπο.

Είναι λοιπόν το F ένα και μόνο δέντρο και μάλιστα παράγει το G και μένει να δειχτεί ότι το F είναι επιπλέον και ελάχιστο δέντρο που παράγει το G. Ας είναι λοιπόν T ένα ελάχιστο δέντρο από αυτά που παράγουν το G που το επιλέγουμε ούτως ώστε να συμφωνεί με το F για το μέγιστο δυνατό διάστημα Το διάστημα συμφωνίας είναι ο χρόνος μέχρι να βρεθεί η πρώτη ακμή (με τη διάταξη του S) η οποία ανήκει στο ένα αλλά όχι στο άλλο. Αν όλες οι ακμές τους ταυτίζονται τότε έχουμε $F = T$ και άρα το F είναι και αυτό ελάχιστο. Άρα μπορούμε να υποθέσουμε ότι υπάρχει μια ακμή e που είτε περιέχεται στο F αλλά όχι στο T είτε περιέχεται στο T αλλά όχι στο F. Ας πάρουμε να είναι η e η πρώτη από τις ακμές που κοιτάει ο αλγόριθμος για την οποία συμβαίνει αυτό.

Η πρώτη παρατήρηση είναι ότι

$$e \in F \setminus T. \tag{5.5}$$

Ο λόγος είναι ότι όταν μια ακμή εξετάζεται από τον αλγόριθμο του Kruskal και απορρίπτεται αυτό συνεπάγεται ότι εκείνη τη στιγμή τα δύο άκρα της είναι ήδη συνδεδεμένα στο F. Αλλά, μέχρι εκείνη τη στιγμή το T συμφωνεί με το F, άρα τα δύο άκρα της e είναι ήδη συνδεδεμένα και στο T, πράγμα που απαγορεύει στην e να ανήκει στο T αφού αυτό είναι δέντρο. Άρα η ακμή αυτή δεν απορρίπτεται από τον αλγόριθμο και ισχύει η (5.5).



Σχήμα 5.27: Βοηθητικό σχήμα για την απόδειξη του Θεωρήματος 5.3

Ας εστιάσουμε την προσοχή μας στη χρονική στιγμή που εξετάζεται από τον αλγόριθμο η ακμή e και ας είναι F_1 και F_2 τα δύο δέντρα του (τρέχοντος) F τα οποία η ακμή αυτή ενώνει. Αφού $e \notin T$ αν την προσθέσουμε στο T δημιουργείται ένας κύκλος C και έπεται ότι υπάρχει κάποια από τις ακμές του $C \setminus \{e\}$, έστω η f, που έχει βάρος

$$w(f) \geq w(e).$$

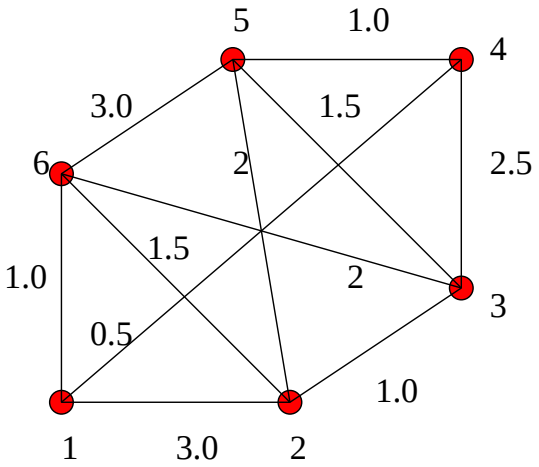
Αυτό συμβαίνει γιατί στην αντίθετη περίπτωση όλες οι ακμές του $C \setminus \{e\}$ θα είχαν εξεταστεί από τον αλγόριθμο πριν από την e, και, λόγω της συμφωνίας μεταξύ F και T ως εκείνη τη στιγμή, και επειδή οι ακμές του $C \setminus \{e\}$ ανήκουν όλες στο T, έπεται ότι θα ανήκουν και στο F, πράγμα ασυμβίβαστο με το ότι η e συνδέει δύο διαφορετικές συνεκτικές συνιστώσες F_1 και F_2. (Δείτε το Σχήμα 5.27.)

Θεωρούμε τώρα το δέντρο

$$T' = T \cup \{e\} \setminus f.$$

Αυτό το δέντρο είναι επίσης ελάχιστο και επίσης συμφωνεί με το F για παραπάνω χρόνο απ' ότι το T, άτοπο διότι το T είχε υποτεθεί ότι μεγιστοποιεί αυτό το χρόνο συμφωνίας. Άρα $F = T$ και το F είναι ελάχιστο.

■



Σχήμα 5.28: Ένα γράφημα με βάρη

✏ **5.41**

Εφαρμόστε με το χέρι τον αλγόριθμο του Kruskal στο γράφημα του Σχήματος 5.28 και βρείτε ένα ελάχιστο δέντρο που το παράγει.

✏ **5.42**

Υλοποιήστε τον αλγόριθμο του Kruskal στην αγαπημένη σας γλώσσα προγραμματισμού με τρόπο ώστε ο χρόνος εκτέλεσης να είναι της τάξης του $m \log m$, όπου m είναι το πλήθος των ακμών (που αναγκαστικά είναι τουλάχιστον $n-1$, όπου n είναι το πλήθος των κορυφών, μια και το γράφημα υποτίθεται συνεκτικό. Εξηγήστε το χρόνο εκτέλεσης του αλγορίθμου.

Ο αλγόριθμος του Kruskal ανήκει σ'εκείνη την κατηγορία αλγορίθμων που ονομάζονται «μυωπικοί» (greedy) μια και προσπαθούν να πετύχουν μια συνολική βελτιστοποίηση (στην περίπτωσή μας την εύρεση ενός ελάχιστου δέντρου) βελτιστοποιώντας, κατά τη διάρκεια της εκτέλεσης τους, κάθε επιλογή που έχουν να κάνουν με κάποια κριτήρια «της στιγμής». Τέτοιοι αλγόριθμοι σπανίως βελτιστοποιούν το συνολικό πρόβλημα, και αυτός ο αλγόριθμος για ελάχιστα δέντρα είναι μια από τις εξαιρέσεις όπου αποδεδειγμένα επιτυγχάνεται συνολική βελτιστοποίηση.

5.8 Ο αλγόριθμος Floyd-Warshall για εύρεση αποστάσεων πάνω σε γραφήματα

Εδώ θα περιγράψουμε ένα αλγόριθμο που βρίσκει όλες τις αποστάσεις ανάμεσα σε όλα τα ζευγάρια κορυφών, σε ένα γράφημα G με (μη αρνητικά) βάρη στις ακμές του. Πρέπει να τονίσουμε ότι το πρόβλημα που λύνουμε εδώ αλγοριθμικά είναι το πρόβλημα των αποστάσεων από «οποιαδήποτε σε οποιαδήποτε» κορυφή. Στο τέλος του αλγορίθμου δηλ. θα μπορούμε να απαντήσουμε άμεσα (σε σταθερό χρόνο, όπως λέμε) σε κάθε ερώτημα «ποια είναι η απόσταση ανάμεσα στις κορυφές i και j του γραφήματος;».

Αν δε μας ενδιέφερε αυτή η γενικότητα αλλά θέλαμε, π.χ., να γνωρίζουμε, μετά το πέρας του αλγορίθμου, όλες τις αποστάσεις από την κορυφή 1 προς όλες τις άλλες, τότε θα χρησιμοποιούσαμε διαφορετικό αλγόριθμο. Ο αλγόριθμος που δίνουμε σε αυτή την παράγραφο θα αποτελούσε «overkill» για ένα τέτοιο ερώτημα: υπολογίζει πολλά αδιάφορα πράγματα.

Θεωρούμε, ως συνήθως, το σύνολο κορυφών του γραφήματος να είναι το $[n] = \{1, 2, \ldots, n\}$ και γράφουμε $w(i, j)$ για το βάρος της ακμής (i, j) (το οποίο συμφωνούμε να θεωρούμε $+\infty$ αν η ακμή αυτή δεν υπάρχει).

Ο παρακάτω αλγόριθμος τροποποιεί σε κάθε επανάληψή του τον $n \times n$ πίνακα A ο οποίος παίρνει αρχικές τιμές στο βήμα 1 και ενημερώνεται n φορές στο βήμα 3.

Αλγόριθμος Floyd–Warshall

1. Θέτουμε $A_{ij}^{(0)} = w(i,j)$, για $i,j = 1,\ldots,n$.
2. Επαναλαμβάνουμε για $k = 1,2,\ldots,n$ το παρακάτω βήμα.
3. $A_{ij}^{(k)} = \min\left\{A_{ij}^{(k-1)},\ A_{ik}^{(k-1)} + A_{kj}^{(k-1)}\right\}$, για $i,j = 1,\ldots,n$.

Θεώρημα 5.4
Στο τέλος του προηγούμενου αλγορίθμου η απόσταση ανάμεσα στις κορυφές i και j είναι ίση με $A_{ij}^{(n)}$.

Απόδειξη

Θα δείξουμε με επαγωγή ως προς το k ότι $A_{ij}^{(k)}$ ισούται με $L_{ij}^{(k)}$ = το μήκος του ελάχιστου μονοπατιού από το i στο j το οποίο όμως χρησιμοποιεί ενδιάμεσες κορυφές μόνο από το σύνολο $\{1,\ldots,k\}$.

Για $k = 0$ το παραπάνω σύνολο είναι κενό και ο ισχυρισμός σημαίνει ότι $A_{ij}^{(0)}$ ισούται με το βάρος της πλευράς (i,j) μια και το σύνολο των μονοπατιών από το i στο j που *δε* χρησιμοποιούν καμία ενδιάμεση κορυφή αποτελείται από την ακμή (i,j) και μόνο. Άρα ο ισχυρισμός είναι αληθής για $k = 0$.

Υποθέτουμε τώρα ότι ο ισχυρισμός ισχύει μέχρι και για $k-1$, θεωρούμε ένα ελάχιστο μονοπάτι από το i στο j που χρησιμοποιεί ενδιάμεσες κορυφές μόνο από το σύνολο $\{1,\ldots,k\}$, και ξεχωρίζουμε δύο περιπτώσεις.

(α) Το ελάχιστο αυτό μονοπάτι *δε* χρησιμοποιεί την κορυφή k.

(β) Χρησιμοποιεί την κορυφή k.

Στην πρώτη περίπτωση έχουμε φυσικά $L_{ij}^{(k)} = L_{ij}^{(k-1)}$.

Εστω ότι ισχύει το (β). Μπορούμε εύκολα να δείξουμε ότι όποιο και να είναι το ελάχιστο μονοπάτι από το i στο j περιέχει το k ακριβώς μια φορά (αν το περιέχει δυο ή παραπάνω μπορούμε να το μικρύνουμε το μονοπάτι παραλείποντας ένα κομμάτι ανάμεσα σε δύο εμφανίσεις του k). Επίσης, το κομμάτι του μονοπατιού από το i στο k είναι ένα ελάχιστο μονοπάτι από το i στο k που χρησιμοποιεί ενδιάμεσες κορυφές από το σύνολο $\{1,\ldots,k-1\}$. Αρα το μήκος του είναι $L_{ik}^{(k-1)}$ και, ομοίως, το μήκος του μονοπατιού από το k στο j είναι $L_{kj}^{(k-1)}$. Το συνολικό μήκος του μονοπατιού είναι λοιπόν σ'αυτή την περίπτωση

$$L_{ij}^{(k)} = L_{ik}^{(k-1)} + L_{kj}^{(k-1)}.$$

Επίσης, σε κάθε περίπτωση, έχουμε τις ανισότητες

$$L_{ij}^{(k)} \le L_{ij}^{(k-1)} \ \ \kappa\alpha\iota \ \ L_{ij}^{(k)} \le L_{ik}^{(k-1)} + L_{kj}^{(k-1)},$$

η πρώτη από τον ορισμό του του συμβόλου L και μόνο και η δεύτερη παρατηρώντας ότι μπορούμε να πάμε από το i στο j (με ενδιάμεσους από το $[k]$) ακολουθώντας πρώτα ένα ελάχιστο μονοπάτι από το i στο k και μετά ένα ελάχιστο μονοπάτι από το k στο j (με ενδιάμεσους από το $[k-1]$).

Από τα παραπάνω προκύπτει ότι

$$L_{ij}^{(k)} = \min\left\{L_{ij}^{(k-1)}, L_{ik}^{(k-1)} + L_{kj}^{(k-1)}\right\}$$

και άρα, από τον τρόπο υπολογισμού των πινάκων $A^{(k)}$, έχουμε $A_{ij}^{(k)} = L_{ij}^{(k)}$, για κάθε $i,j = 1,\ldots,n$, $k = 0,\ldots,n$.

■

Μπορεί κανείς εύκολα να δεί ότι ο αλγόριθμος Floyd-Warshall που περιγράψαμε παίρνει περίπου n^3 υπολογιστικά βήματα για να τελειώσει.

✏ **5.43**

Πόσες πράξεις (προσθέσεις και πολλαπλασιασμούς) χρειάζεται ο αλγόριθμος Floyd-Warshall για να υπολογίσει το ζητούμενο; Πόσο χώρο (θέσεις για αριθμούς) χρειάζεται ο αλγόριθμος αυτός;

✏ **5.44**

Γράψτε ένα πρόγραμμα που θα υλοποιεί τον αλγόριθμο Floyd-Warshall και εφαρμόστε τον στο γράφημα του Σχήματος 5.28.

Βιβλιογραφία Κεφαλαίου

[1] Peter J Cameron. *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, 1994.

[2] Reinhard Diestel. *Graph theory*. 2005.

[3] Chung Laung Liu and CL Liu. *Elements of discrete mathematics*. McGraw-Hill New York, 1985.

[4] Richard P Stanley. *Enumerative combinatorics*. 1986.

Κεφάλαιο 6

Διμερή γραφήματα και ταιριάσματα

Κύριες βιβλιογραφικές αναφορές για αυτό το Κεφάλαιο είναι οι C. L. Liu and C. Liu 1985, Cameron 1994, Diestel 2005 και Stanley 1986.

6.1 Διμερή γραφήματα

Η κλάση των διμερών γραφημάτων κωδικοποιεί φυσιολογικά σχέσεις ανάμεσα σε δύο διαφορετικούς πληθυσμούς. Για παράδειγμα ας υποθέσουμε ότι έχουμε δύο ξένα πεπερασμένα σύνολα: το A, που είναι ένα σύνολο δασκάλων, και το B, που είναι ένα σύνολο μαθητών. Ορίζουμε ένα γράφημα με σύνολο κορυφών το $V = A \cup B$ το οποίο θα κωδικοποιεί τη σχέση διδασκαλίας, βάζουμε δηλ. μια ακμή ανάμεσα σε δύο κορυφές $u, v \in V$ αν και μόνο αν το u διδάσκει το v ή αντίστροφα. Είναι φανερό ότι όλες οι ακμές στο γράφημα αυτό συνδέουν μεταξύ τους μια κορυφή του A και μια του B. Δεν υπάρχουν δηλ. ακμές που να συνδέουν ανάμεσά τους δύο κορυφές του A ή δύο του B. Μία άλλη περίπτωση, αρκετά κοινή στην πράξη, είναι αυτή όπου έχουμε ένα γράφημα που περιγράφει τη σχέση ανάμεσα σε εξυπηρετητές (servers) και εξυπηρετούμενους (clients).

Ορισμός 6.1
(Διμερές γράφημα) *Ενα γράφημα $G = (V, E)$ θα ονομάζεται* διμερές *αν υπάρχει μια διαμέριση των κορυφών*

$$V = A \cup B, \quad \mu\epsilon\ A \cap B = \emptyset,$$

τέτοια ώστε οι γείτονες κάθε κορυφής του A ανήκουν στο B (το οποίο συνεπάγεται ότι και οι γείτονες κάθε κορυφής του B ανήκουν στο A). Δεν υπάρχουν δηλ. ακμές από το A στο A ή από το B στο B.

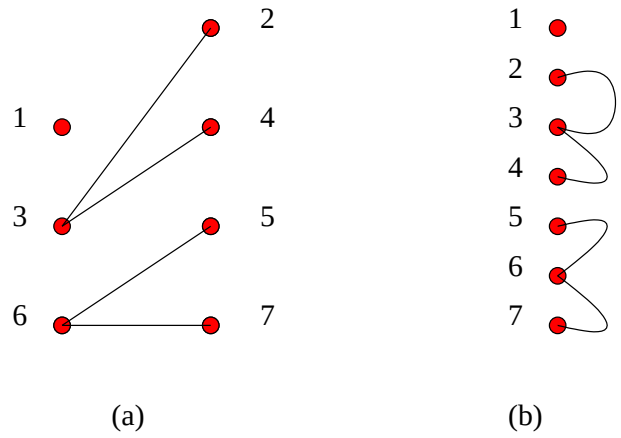
Παράδειγμα 6.1
Σε ένα σύνολο ανθρώπων η σχέση του γάμου ορίζει ένα διμερές γράφημα. Αν έχουμε δηλ. ένα γράφημα με σύνολο κορυφών V κάποιο σύνολο ανθρώπων, και βάλουμε μια ακμή ανάμεσα σε δύο κορυφές αν αυτές αντιπροσωπεύουν συζύγους, τότε το γράφημα είναι διμερές με σύνολο κορυφών A το σύνολο των γυναικών και σύνολο κορυφών B το σύνολο των ανδρών.

Παρατήρηση 6.1
Τα διμερή γραφήματα τα σχεδιάζουμε συνήθως (αλλά όχι πάντα) με τις δύο ομάδες (A και B) των κορυφών τους σαφώς χωρισμένες, συνήθως σε αριστερά και δεξιά. Για παράδειγμα, το γράφημα στο Σχ. 6.1(a) είναι διμερές με

$$A = \{1, 3, 6\}, \quad B = \{2, 4, 5, 7\}.$$

Δεν είναι πάντα προφανές, απλά κοιτώντας ένα γράφημα, αν είναι αυτό διμερές ή όχι. Το γράφημα στο Σχ. 6.1(b) είναι το ίδιο με το γράφημα στο (a) αλλά πρέπει κανείς να σκεφτεί για να δεί ότι όντως είναι διμερές.

Παρατήρηση 6.2
Παρατηρήστε ότι η διαμέριση $V = A \cup B$ δεν είναι μοναδική, μια και θα μπορούσαμε να είχαμε τοποθετήσει, για παράδειγμα, το 1 στο σύνολο B αντί για το A.



Σχήμα 6.1: Ένα διμερές γράφημα, σχεδιασμένο με δύο τρόπους

✏ **6.1**
Δείξτε ότι ένα γράφημα G είναι διμερές αν και μόνο αν κάθε συνεκτική συνιστώσα του G είναι διμερές γράφημα.

✏ **6.2**
Βρείτε μια μέθοδο για να αποφασίζετε αν ένα τυχόν απλό γράφημα είναι διμερές ή όχι.

Κατ' αρχήν, αρκεί να βρούμε μια τέτοια μέθοδο που δουλεύει για συνεκτικά γραφήματα (σύμφωνα με την Άσκηση 6.1). Για ένα συνεκτικό γράφημα $G = (V, E)$ επιλέγουμε αυθαίρετα μια κορυφή του u και ορίζουμε τα σύνολα

$$V(k) = \{v \in V : \ d(u, v) = k\}, \quad k = 0, 1, \ldots, \operatorname{diam} G,$$

τα οποία διαμερίζουν το σύνολο κορυφών V. Το σύνολο $V(k)$ απαρτίζεται από εκείνες τις κορυφές του G που απέχουν απόσταση ακριβώς k από την κορυφή u. Δείξτε ότι το G είναι διμερές αν και μόνο αν για κάθε ακμή

$$ab, \quad \mu\epsilon\ a \in V(i),\ b \in V(j),$$

έχουμε $i \equiv j$ mod 2, είναι δηλ. τα i, j είτε και τα δύο άρτια είτε και τα δύο περιττά.

Θεώρημα 6.1
Όλα τα δέντρα είναι διμερή γραφήματα.

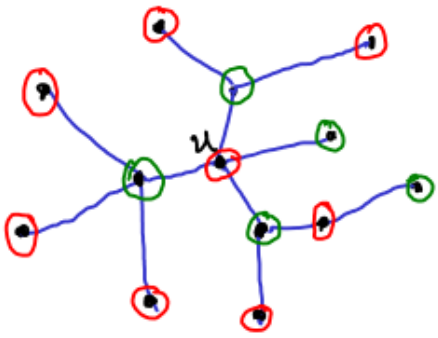
Απόδειξη

Η απόδειξη είναι με επαγωγή ως προς το $n = |V|$. Αν $n = 1$, τότε το μοναδικό δέντρο είναι αυτό με μια κορυφή u και καμιά ακμή. Ορίζουμε τότε το διαμερισμό του συνόλου $V = \{u\}$ στα σύνολα $A = \{u\}$ και $B = \emptyset$.

Για το επαγωγικό βήμα, υποθέτουμε ότι η πρόταση ισχύει αν το δέντρο έχει το πολύ $n - 1$ κορυφές και παίρνουμε ένα δέντρο T με n κορυφές. Θέλουμε να δείξουμε ότι είναι διμερές. Γνωρίζουμε όμως (δείτε τον ισχυρισμό μέσα στην απόδειξη του Θεωρήματος 5.2) ότι κάθε δέντρο έχει μια κορυφή βαθμού 1. Έστω u μια τέτοια κορυφή του δέντρου T, και v ο μοναδικός γείτονάς της. Αν από το T αφαιρέσουμε την κορυφή u και την ακμή uv, τότε το γράφημα που προκύπτει, έστω T' είναι και πάλι δέντρο (αφού εξακολουθεί να παραμένει συνεκτικό γράφημα, χωρίς κύκλους) με $n - 1$ κορυφές. Από την επαγωγική μας υπόθεση έπεται ότι το T' είναι διμερές με σύνολα κορυφών τα A' και B' (όλες οι ακμές του T' δηλ. πάνε από το A' στο B'). Η κορυφή v ανήκει σε ένα από τα δύο αυτά σύνολα, έστω στο A'.

Ισχυριζόμαστε τώρα ότι το δέντρο T είναι διμερές γράφημα με σύνολα κορυφών τα $A = A'$ και $B = B' \cup \{u\}$. Για να το ελέγξουμε αυτό, και εφόσον γνωρίζουμε ότι δεν υπάρχουν ακμές από το A'

στο B', αρκεί να ελέγκσουμε ότι δεν υπάρχουν ακμές από το u προς κάποια κορυφή του B'. Αυτό όμως είναι προφανές αφού το u έχει μόνο ένα γείτονα, το v, ο οποίος είναι στο A.
■



Σχήμα 6.2: Ένας τρόπος να βρούμε τα δύο σύνολα A και B που ορίζουν ένα δέντρο ως διμερές γράφημα είναι να ξεκινήσουμε από μια αυθαίρετη κορυφή u του δέντρου την οποία και χρωματίζουμε κόκκινη, μετά να χρωματίσουμε τους γείτονές της πράσινους, μετά να χρωματίσουμε τους αχρωμάτιστους γείτονες των τελευταίων κορυφών που χρωματίσαμε με το άλλο χρώμα κλπ.

✏ **6.3**
Αν ένα γράφημα είναι διμερές τότε και κάθε υπογράφημά του είναι.

✏ **6.4**
Ο κύκλος C_n είναι το γράφημα με σύνολο κορυφών το $\{1, 2, \ldots, n\}$ και σύνολο ακμών το

$$E = \{(1, 2), (2, 3), \ldots, (n - 1, n), (n, 1)\}.$$

Δείξτε ότι το C_n είναι διμερές γράφημα αν και μόνο αν το n είναι άρτιο.

✏ **6.5**
Το πλήρες διμερές γράφημα με m και n κορυφές, που το συμβολίζουμε με K_{mn} είναι ένα διμερές γράφημα με σύνολα κορυφών $A = \{a_1, \ldots, a_m\}$ και $B = \{b_1, \ldots, b_n\}$, όπου το σύνολο των ακμών είναι το μέγιστο δυνατό.

Δείτε στο Σχήμα 5.8 π.χ. το γράφημα $K_{4,3}$.

1. *Πόσες ακμές έχει το K_{mn};*
2. *Για ποιες τιμές των m και n είναι το K_{mn} κανονικό; (Θυμίζουμε ότι ένα γράφημα λέγεται κανονικό αν όλες οι κορυφές του έχουν τον ίδιο βαθμό.)*
3. *Περιγράψτε το συμπληρωματικό γράφημα του K_{mn}.* (Συμπληρωματικό *ενός γραφήματος G είναι το γράφημα G' με ίδιο σύνολο κορυφών και τέτοιο ώστε μια ακμή υπάρχει στο G' αν και μόνο αν δεν υπάρχει στο G.) Είναι αυτό διμερές;*

✏ **6.6**
Μπορεί ένα δέντρο να είναι πλήρες διμερές γράφημα; (Δείτε ορισμό στην Άσκηση 6.5.)

Τα διμερή γραφήματα χαρακτηρίζονται από τα μήκη των κυκλωμάτων τους:

Θεώρημα 6.2
Ένα γράφημα είναι διμερές αν και μόνο αν όλα τα κυκλώματά του έχουν άρτιο μήκος.

Απόδειξη

Έστω G διμερές γράφημα και C κύκλωμα σε αυτό:

$$C: \ u_1 \to u_2 \to \cdots \to u_n \to u_1.$$

Το μήκος του C είναι n και θέλουμε να δείξουμε ότι αυτό είναι άρτιο. Μπορούμε να υποθέσουμε ότι το u_1 ανήκει στο σύνολο κορυφών A. Άρα το u_2 ανήκει στο σύνολο κορυφών B, το u_3 ανήκει πάλι στο A, κλπ. Δηλ. τα u_j με άρτιο j ανήκουν στο B και αυτά με περιττό j στο A. Όμως το u_n είναι γείτονας του u_1, άρα ανήκει στο B, το οποίο συνεπάγεται ότι το n είναι άρτιο.

Αντίστροφα, έστω G ένα γράφημα, με σύνολο κορυφών V, στο οποίο όλα τα κυκλώματα έχουν άρτιο μήκος. Υποθέτουμε πρώτα ότι το G είναι συνεκτικό και σταθεροποιούμε μια κορυφή του u. Ορίζουμε

$$A = \{v \in V: \ d(u,v) \ \alpha\rho\tau\iota o\}$$

και

$$B = V \setminus A.$$

Δείχνουμε ότι το G είναι διμερές με σύνολα κορυφών τα A και B. Γι' αυτό αρκεί να δείξουμε ότι είναι αδύνατο να υπάρχει ακμή ανάμεσα σε δύο κορυφές του A ή ανάμεσα σε δύο κορυφές του B. Έστω a_1 και a_2 δύο κορυφές του A (επιχειρηματολογούμε τελείως όμοια για δύο κορυφές του B) και ας υποθέσουμε, αντίθετα με αυτό που θέλουμε να αποδείξουμε, ότι υπάρχει στο G η ακμή a_1a_2. Έστω π_1 και π_2 δύο ελάχιστα μονοπάτια στο G από την u στις κορυφές a_1 και a_2. Θεωρούμε τον κύκλο C που απαρτίζεται από το π_1 ακολουθούμενο από την ακμή a_1a_2 και τέλος από το π_2 διανυμένο με ανάποδη σειρά. Το μήκος του C είναι

$$|C| = |\pi_1| + 1 + |\pi_2|,$$

που είναι φανερό ότι είναι περιττός αριθμός, πράγμα άτοπο.

Έχουμε λοιπόν δείξει τη συνεπαγωγή «άρτια κυκλώματα συνεπάγεται διμερές γράφημα» στην περίπτωση που το G είναι συνεκτικό. Αν το G δεν είναι συνεκτικό παρατηρούμε ότι κάθε συνεκτική συνιστώσα του είναι διμερής, άρα και το ίδιο το G (δείτε Άσκηση 6.1).

■

✏ **6.7**

Ο χρωματικός αριθμός *ενός γραφήματος G, που συμβολίζεται με $\chi(G)$, είναι ο ελάχιστος ακέραιος k τέτοιος ώστε να μπορεί κανείς με k διαφορετικά χρώματα να χρωματίσει τις κορυφές του G, με τέτοιο τρόπο ώστε αν δύο κορυφές συνδέονται με ακμή τότε να έχουν διαφορετικά χρώματα. Για παράδειγμα ο χρωματικός αριθμός ενός τριγώνου (K_3) είναι 3. Δείξτε ότι ένα γράφημα G είναι διμερές αν και μόνο αν $\chi(G) \leq 2$.*

✏ **6.8**

Αν $A = \{a_1, \ldots, a_m\}$ και $B = \{b_1, \ldots, b_n\}$, πόσα διμερή γραφήματα υπάρχουν με σύνολα κορυφών τα A και B;

Κάθε μια από τις δυνατές ακμές από το A στο B μπορεί να επιλεγεί ως ακμή ή όχι.

✏ **6.9**

Αν $A = \{a_1, \ldots, a_m\}$ και $B = \{b_1, \ldots, b_n\}$, για ποιες τιμές των m, n και r υπάρχει r-κανονικό γράφημα με σύνολα κορυφών τα A και B;

Μετρήστε κατ' αρχήν τις ακμές ενός τέτοιου γραφήματος από τη μεριά του A. Αφού για κάυε κορυφή του A έχουμε r ακμές που φεύγουν από αυτό θα έχει συνολικά $m \cdot r$ ακμές ένα τέτοιο γράφημα. Κάντε το ίδιο από την πλευρά του B.

Για την αντίστροφη κατεύθυνση θα πρέπει να δώσετε μια κατασκευή.

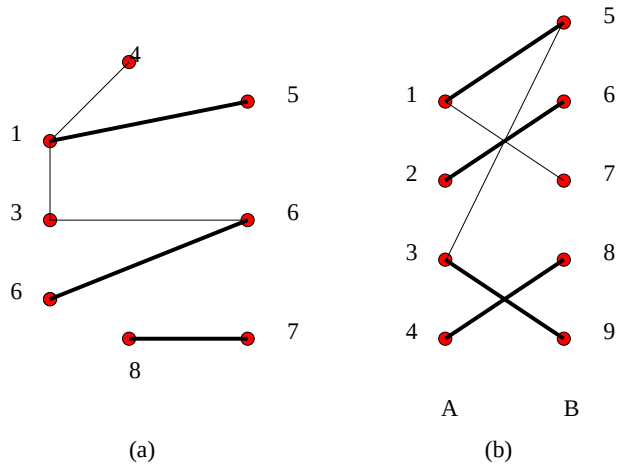
✏ **6.10**

Τι μορφή έχει ο πίνακας συνδεσμολογίας ενός διμερούς γραφήματος (μετά από κατάλληλη αρίθμηση των κορυφών του);

6.2 Ταιριάσματα σε διμερή γραφήματα

Μια πολύ χρήσιμη έννοια είναι η έννοια του ταιριάσματος σε ένα γράφημα.

Ορισμός 6.2
(Ανεξάρτητες ακμές, Ταιριάσματα) *Δύο ακμές λέγονται* ανεξάρτητες *αν δεν έχουν κοινή κορυφή. Ένα σύνολο ανεξαρτήτων ακμών M σε ένα γράφημα λέγεται ταίριασμα (matching). Αν το γράφημα είναι διμερές με σύνολα κορυφών A και B τότε ένα ταίριασμα M λέγεται* πλήρες ταίριασμα *του A (ομοίως για το B) αν κάθε κορυφή του A περιέχεται σε κάποια ακμή του M.*



Σχήμα 6.3: Οι ακμές με έντονη γραμμή αποτελούν ταίριασμα

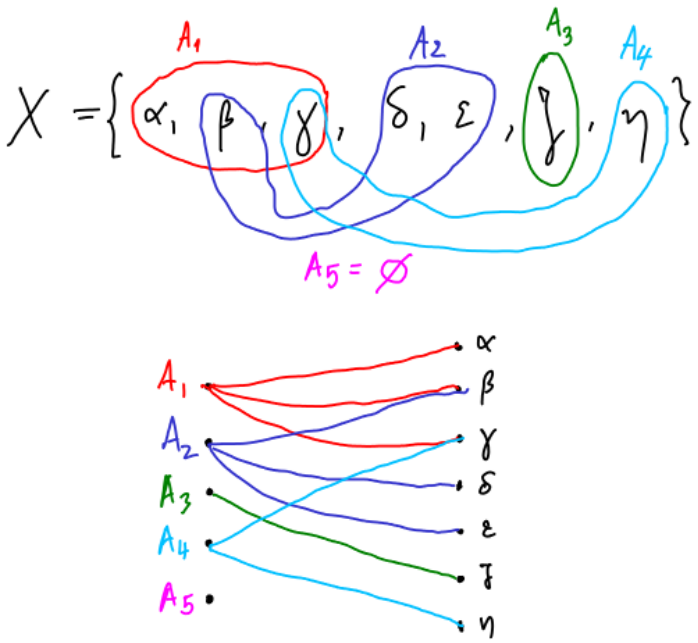
Παράδειγμα 6.2
Στο Σχ. 6.3(a) το σύνολο των ακμών που έχουν σχεδιαστεί έντονα αποτελεί ένα ταίριασμα. Στο Σχ. 6.3(b) έχουμε ένα διμερές γράφημα με ένα ταίριασμα του πλήρες συνόλου κορυφών A (αριστερές κορυφές). Το ταίριασμα αυτό δεν αποτελεί πλήρες ταίριασμα του B αφού η κορυφή 9 του B δεν «καλύπτεται» από ακμή του ταιριάσματος.

Παράδειγμα 6.3
Ας υποθέσουμε ότι έχουμε προκηρύξει κάποιες θέσεις εργασίας $J_1, \ldots, J_n$ και ότι έχουν κάνει αίτηση γι' αυτές κάποιοι υποψήφιοι $C_1, \ldots, C_m$, με $m \geq n$. Δεν έχει κατ' ανάγκην κάνει αίτηση ο κάθε υποψήφιος για όλες τις θέσεις, αλλά κάθε υποψήφιος έχει κάνει αίτηση για κάποιες από τις προσφερόμενες θέσεις. Σκοπός μας είναι να γεμίσουμε όλες τις θέσεις εργασίας. Δε μπορούμε φυσικά να προσλάβουμε για μια θέση εργασίας κάποιον που δεν έχει κάνει αίτηση γι' αυτή. Φτιάχνουμε ένα διμερές γράφημα με σύνολα κορυφών $A = \{J_1, \ldots, J_n\}$ και $B = \{C_1, \ldots, C_m\}$ και βάζουμε μια ακμή ανάμεσα στις κορυφές J_k και C_l αν και μόνο αν ο υποψήφιος C_l έχει κάνει αίτηση για τη θέση J_k. Είναι φανερό τώρα ότι μπορούμε να γεμίσουμε όλες τις θέσεις εργασίας αν και μόνο αν υπάρχει πλήρες ταίριασμα του A στο γράφημα αυτό.

✏ **6.11**
Αν ένα διμερές γράφημα με σύνολα κορυφών A και B έχει πλήρες ταίριασμα του A τότε $|B| \geq |A|$.

Έστω ένα πεπερασμένο σύνολο X και σύστημα $A_1, \ldots, A_n$ υποσυνόλων του. Υπάρχει ένας πολύ φυσιολογικός τρόπος να αντιστοιχίσουμε σε αυτό το σύστημα υποσυνόλων ένα διμερές γράφημα:

σύνολο αριστερών κορυφών είναι τα σύνολα $A_1, \ldots, A_n$ και σύνολο δεξιών κορυφών είναι το X. Ενώνουμε την αριστερή κορυφή A_i με τη δεξιά κορυφή x αν και μόνο αν $x \in A_i$.



Παρατήρηση 6.3Σχήμα 6.4: Ένα σύνολο $X = \{\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta\}$, κάποια υποσύνολά του $A_1, \ldots, A_5$ και το διμερές γράφημα που αντιστοιχεί στο σύστημα αυτό υποσυνόλων του X. Αριστερά (ή δεξιά, δεν έχει σημασία, αλλά πάντως στη μια μεριά μόνο) βάζουμε τα ονόματα των υποσυνόλων, δεξιά τα ονόματα των στοιχείων του X ενώνουμε ένα στοιχείο με ένα υποσύνολο αν και μόνο αν το στοιχείο ανήκει στο υποσύνολο.

Είναι φανερό ότι σε διαφορετικά συστήματα υποσυνόλων του X αντιστοιχούν διαφορετικά διμερή γραφήματα κατασκευασμένα κατά αυτόν τον τρόπο και είναι επίσης φανερό πώς να κατασκευάσουμε ένα σύστημα υποσυνόλων όταν μας δώσουν ένα διμερές γράφημα.

Δείτε το Σχήμα 6.4 για παράδειγμα.

Ορισμός 6.3
Σε ένα διμερές γράφημα, για κάθε σύνολο J αριστερών κορυφών, συμβολίζουμε με $N(J)$ το σύνολο όλων των δεξιών κορυφών που ενώνονται με κάποια κορυφή από το J.

Το αποτέλεσμα που ακολουθεί περιγράφει ακριβώς πότε ένα διμερές γράφημα έχει πλήρες ταίριασμα της μιας πλευράς του.

Θεώρημα 6.3
Σε ένα διμερές γράφημα με σύνολα κορυφών A και B υπάρχει πλήρες ταίριασμα του A αν και μόνο αν για κάθε υποσύνολο $J \subseteq A$ ισχύει

$$|N(J)| \geq |J|. \tag{6.1}$$

Απόδειξη

Το Θεώρημα 6.3 αποτελεί ουσιαστικά μια αναδιατύπωση του Θεωρήματος του Γάμου (Θεώρημα 1.5). Φτιάχνουμε από το διμερές μας γράφημα ένα σύστημα υποσυνόλων του B, όπως στην Παρατήρηση 6.3. Η συνθήκη του Θεωρήματος 6.3 αποτελεί απλά αναδιατύπωση της συνθήκης (1.21) του Hall. Το γράφημά μας έχει πλήρες ταίριασμα του A αν και μόνο αν το σύστημα υποσυνόλων του B που φτιάξαμε έχει σύστημα ξένων αντιπροσώπων, πράγμα που, σύμφωνα με το Θεώρημα του Γάμου, ισχύει ακριβώς όταν ισχύει η συνθήκη του Hall, δηλ. η συνθήκη που διατυπώνεται στο Θεώρημα 6.3.
■

✏ **6.12**
Σε ένα διμερές γράφημα με σύνολα κορυφών A και B ισχύει

$$|N(J)| \geq |J| - 5, \ \ \forall J \subseteq A.$$

Δείξτε ότι υπάρχει ταίριασμα M που να περιέχει τουλάχιστον $|A| - 5$ κορυφές του A.

Προσθέστε 5 κορυφές στο σύνολο B και συνδέσετέ τις με όλες τις κορυφές του A. Το νέο αυτό διμερές γράφημα τώρα ικανοποιεί τη συνθήκη του Hall (6.1). Αφού χρησιμοποιήσετε το Θεώρημα 6.3 θα πρέπει από το συμπέρασμά σας να «ξεφορτωθείτε» τις παραπανίσιες κορυφές που εισαγάγατε προηγουμένως.

Μια εύκολη συνέπεια του θεωρήματος του Γάμου είναι η εξής:

Πόρισμα 6.1
Κάθε κανονικό διμερές γράφημα έχει πλήρες ταίριασμα (και των δύο μεριών του, αναγκαστικά).

Απόδειξη

Εστω ότι το $G = (A \cup B, E)$ είναι r-κανονικό, $r \geq 1$. Θα αποδείξουμε ότι ισχύει η υπόθεση του Θεωρήματος 6.3. Εστω $J \subseteq A$ και E_1 το σύνολο των ακμών που ξεκινούν από κάποια κορυφή του J. Επειδή το G είναι r-κανονικό έχουμε ότι $|E_1| = r|J|$.

Εστω επίσης E_2 το σύνολο των ακμών που καταλήγουν σε κάποια από τις κορυφές του $N(J)$, δηλ. σε κάποιο από τους γείτονες του J. Ξανά έχουμε $|E_2| = r|N(J)|$.

Αλλά προφανώς ισχύει $E_1 \subseteq E_2$. Αρα $r|J| \leq r|N(J)|$, το οποίο συνεπάγεται

$$|N(J)| \geq |J|.$$

■

✏ **6.13**
Αν ένα διμερές γράφημα είναι r-κανονικό δείξτε ότι έχει r ξένα μεταξύ τους πλήρη ταιριάσματα.

Χρησιμοποιήστε το Πόρισμα 6.1. Αφού βρείτε ένα πλήρες ταίρασμα διαγράψτε όλες τις ακμές του από το γράφημά σας. Τι ιδιότητες έχει το γράφημα που απομένει;

✏ **6.14**
Παίρνουμε μια συνηθισμένη τράπουλα (52 φύλλα σε 13 είδη ($A, 2, 3, \ldots, 10, J, Q, K$), από 4 κάθε είδος ($\clubsuit, \spadesuit, \heartsuit, \diamondsuit$)), την ανακατεύουμε και την μοιράζουμε σε 13 σωρούς των 4 φύλλων. (Τα περιεχόμενα των σωρών τα βλέπουμε, τα φύλλα δηλ. κοιτάνε προς τα πάνω.)

Δείξτε ότι είναι πάντα δυνατό να επιλέξουμε ένα φύλλο από κάθε σωρό ώστε στο τέλος να έχουμε ένα φύλλο από κάθε είδος.

Φτιάξτε ένα διμερές γράφημα με τους 13 σωρούς αριστερά και τα 13 είδη δεξιά. Βάλτε μια ακμή από ένα σωρό σε ένα είδος αν και μόνο αν το είδος αυτό εμφανίζεται στο σωρό. Δείξτε ότι το διμερές γράφημα έχει πλήρες ταίριασμα και των δύο πλευρών του. Ένα τέτοιο ταίριασμα σας λέει τι είδος να διαλέξετε από κάθε σωρό.

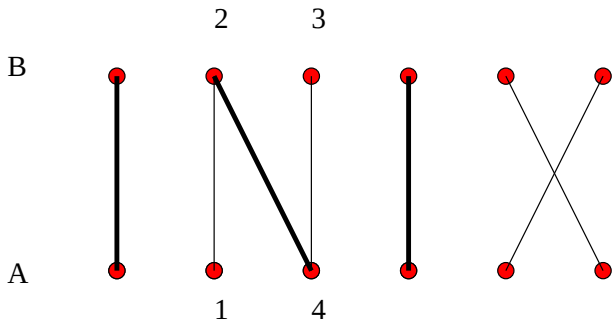
6.3 Μέγιστα ταιριάσματα

Υπάρχουν πολλές ενδιαφέρουσες περιπτώσεις διμερών γραφημάτων που δεν έχουν πλήρη ταιριάσματα του συνόλου κορυφών A. Σέ τέτοια περίπτωση ενδιαφερόμαστε να βρούμε *μέγιστα ταιριάσματα*, ταιριάσματα δηλ. που καλύπτουν το μέγιστο δυνατό αριθμό κορυφών (εναλλακτικά, που έχουν όσο γίνεται περισσότερες ακμές).

Ορισμός 6.4
(Εναλλακτικά μονοπάτια, επαυξάνοντα μονοπάτια) *Μια κορυφή ενός διμερούς γραφήματος που δεν καλύπτεται από κάποια ακμή ενός ταιριάσματος λέγεται* αταίριαστη *(ως προς το ταίριασμα αυτό).*

Σε ένα διμερές γράφημα με σύνολα κορυφών A και B και ένα ταίριασμα M ένα μονοπάτι, χωρίς επαναλαμβανόμενες ακμές, που αρχίζει από μια αταίριαστη κορυφή του A και περιέχει εναλλακτικά ακμές από το $E \setminus M$ και το M, λέγεται εναλλακτικό μονοπάτι.

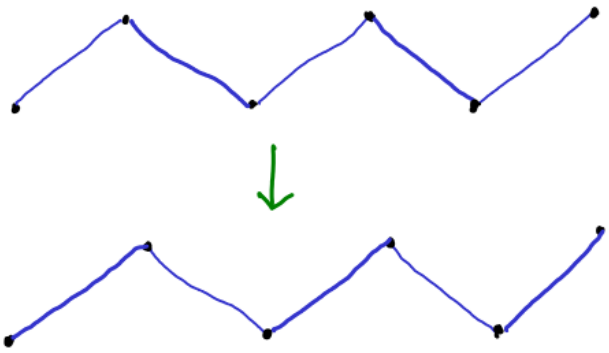
Αν ένα εναλλακτικό μονοπάτι τελειώνει σε μια αταίριαστη κορυφή του B τότε λέγεται επαυξάνον μονοπάτι.



Σχήμα 6.5: Το μονοπάτι 1243 είναι επαυξάνον για το σημειωμένο ταίριασμα

Παράδειγμα 6.4
Στο Σχ. 6.5 το μονοπάτι 1243 είναι επαυξάνον για το ταίριασμα που έχει σημειωθεί με έντονες γραμμές.

Παρατήρηση 6.4



Σχήμα 6.6: Ένα επαυξάνον μονοπάτι (πάνω). Οι έντονες ακμές είναι στο ταίριασμα M. Αν αφαιρέσουμε τις ακμές αυτές από το M και προσθέσουμε στο M τις υπόλοιπες ακμές του μονοπατιού τότε το ταίριασμά μας κερδίζει μια ακμή

Τα επαυξάνοντα μονοπάτια είναι σημαντικά γιατί η ύπαρξη ενός τέτοιου μονοπατιού συνεπάγεται την ύπαρξη ενός μεγαλύτερου ταιριάσματος από το υπάρχον. Πράγματι, σε ένα επαυξάνον μονοπάτι οι ακμές είναι εναλλακτικά εκτός του M, από το M, εκτός του M, κ.ο.κ., και τελειώνουν με μια ακμή εκτός του M, μια και η τελευταία κορυφή του μονοπατιού είναι στο B και αταίριαστη στο ταίριασμα M. Αν λοιπόν αφαιρέσουμε από το M τις ακμές του που συμμετέχουν σε ένα επαυξάνον μονοπάτι π και προσθέσουμε στο M τις ακμές του π που δεν ανήκαν στο M, παίρνουμε ένα άλλο σύνολο ακμών M' που είναι μεγαλύτερο του M κατά μία ακμή. Το σημαντικό εδώ είναι ότι και το M' είναι ταίριασμα (Άσκηση 6.15 παρακάτω), άρα, χρησιμοποιώντας το π καταφέραμε να αυξήσουμε το μέγεθος του δοθέντος ταιριάσματος.

Δείτε το Σχήμα 6.6 και το Παράδειγμα 6.5.

Παράδειγμα 6.5
Στο ταίριασμα του Σχ. 6.5 αν αφαιρέσουμε την ακμή 24 και προσθέσουμε τις 12 και 34 παίρνουμε πάλι ένα ταίριασμα κατά μία ακμή μεγαλύτερο από πριν.

✏ **6.15**
Αποδείξτε τον ισχυρισμό της Παρατήρησης 6.4, ότι το σύνολο ακμών M' είναι ταίριασμα. Συνεπώς αν το M είναι μέγιστο ταίριασμα τότε δεν υπάρχουν επαυξάνοντα μονοπάτια.

Είναι σημαντικό ότι ισχύει και το αντίστροφο της Άσκησης 6.15, και αυτό δεν είναι καθόλου προφανές.

Θεώρημα 6.4
Αν ένα ταίριασμα δεν έχει επαυξάνοντα μονοπάτια τότε είναι μέγιστο ταίριασμα.

Απόδειξη

Έστω M_1 ένα ταίριασμα (ενός διμερούς γραφήματος G, με σύνολα κορυφών A και B) που δεν έχει επαυξάνοντα μονοπάτια, και M_2 ένα μέγιστο ταίρασμα. Θεωρούμε το γράφημα G' με σύνολο ακμών το $M_1 \triangle M_2$ (το σύνολο αυτό είναι η *συμμετρική διαφορά* των M_1 και M_2, οι ακμές εκείνες του G δηλ. που ανήκουν σε ακριβώς ένα από τα σύνολα M_1 και M_2).

Επειδή τα M_1 και M_2 είναι ταιριάσματα έπεται ότι οι κορυφές του G' έχουν όλες βαθμό 0, 1 ή 2 (στο G', όχι στο G). Αυτό ισχύει γιατί αν μια κορυφή του G' έχει βαθμό 3 ή περισσότερο τότε υπάρχουν είτε δύο ακμές του M_1 είτε δύο ακμές του M_2 που καταλήγουν στην κορυφή αυτή, πράγμα που αντιφάσκει με τον ορισμό του ταιριάσματος που απαιτεί όλες οι ακμές του ταιριάσματος να μη μοιράζονται καμία κορυφή.

Από αυτό προκύπτει ότι κάθε συνεκτική συνιστώσα του G' είναι είτε ένας κύκλος είτε ένα μονοπάτι (ενδεχομένως μήκους 0, μια μόνη κορυφή δηλαδή). Και στις δύο αυτές περιπτώσεις οι ακμές σε κάθε συνεκτική συνιστώσα προέρχονται εναλλάξ από το M_1 και το M_2. Όταν η συνιστώσα είναι κύκλος χρησιμοποιούνται σε αυτή ίσο πλήθος ακμών από το M_1 και το M_2. Όταν η συνιστώσα δεν είναι κύκλος αλλά μονοπάτι, ο μόνος τρόπος να εμφανίζονται σε αυτή λιγότερες M_1-ακμές απ' ότι M_2-ακμές είναι το μονοπάτι αυτό να αρχίζει και να τελειώνει με M_2-ακμή πράγμα που θα σήμαινε ότι το μονοπάτι αυτό θα ήταν επαυξάνον για το ταίριασμα M_1, με ενδεχόμενη εναλλαγή των ρόλων των πλευρών A και B.

Επειδή έχουμε υποθέσει ότι επαυξάνοντα μονοπάτια δεν υπάρχουν έπεται ότι και σε αυτή την περίπτωση (η συνιστώσα είναι μονοπάτι καί όχι κύκλος) χρησιμοποιούνται τουλάχιστον τόσες M_1-ακμές όσες και M_2. Και αφού το M_2 είναι μέγιστο ταίριασμα έπεται ότι το πλήθος ακμών του M_1 είναι ίσο με αυτό του M_2 και άρα είναι κι αυτό μέγιστο, όπως έπρεπε να δείξουμε.
■

Παρατήρηση 6.5
Λόγω του Θεωρήματος 6.4 μπορούμε να ακολουθήσουμε την εξής διαδικασία για την εύρεση ενός μέγιστου ταιριάσματος ενός διμερούς γραφήματος: ξεκινάμε από ένα οποιοδήποτε ταίριασμα (π.χ. το κενό) και ψάχνουμε να βρούμε επαυξάνοντα μονοπάτια. Κάθε φορά που βρίσκουμε ένα τέτοιο ακολουθούμε τη διαδικασία της Παρατήρησης 6.4 ώστε να αυξήσουμε κατά μία το σύνολο των ακμών που συμμετέχουν στο ταίριασμά μας. Όταν δε μπορούμε πλέον να βρούμε επαυξάνον μονοπάτι είμαστε σίγουροι, από το Θεώρημα 6.4 ότι έχουμε βρεί ένα μέγιστο ταίριασμα.

Ορισμός 6.5
(Κάλυμμα κορυφών) *Ένα σύνολο κορυφών U σε ένα γράφημα G λέγεται* κάλυμμα κορυφών *του G αν κάθε ακμή του G έχει μια τουλάχιστον κορυφή στο U.*

Παράδειγμα 6.6
Στο Σχ. 6.3(α) το σύνολο $\{1, 6, 8\}$ είναι κάλυμμα κορυφών.

✏ **6.16**
Έστω γράφημα G με ταίριασμα M και κάλυμμα κορυφών U. Δείξτε ότι

$$|U| \geq |M|.$$

Κάθε ακμή του M πρέπει να περιέχει τουλάχιστον μια κορυφή του U. Μπορεί μια τέτοια κορυφή να περιέχεται και σε άλλη ακμή του M;

Θεώρημα 6.5
(König, 1931, και Egerváry, 1931) *Σε ένα διμερές γράφημα το μέγεθος ενός μεγίστου ταιριάσματος ισούται με το μέγεθος ενός ελαχίστου καλύμματος κορυφών.*

Απόδειξη

Έστω G διμερές γράφημα με σύνολα κορυφών τα A και B και M ένα ταίριασμα του G με μέγιστο πλήθος ακμών. Θα κατασκευάσουμε ένα σύνολο κορυφών U, μεγέθους $|U| = |M|$, που θα είναι κάλυμμα κορυφών του G. Αυτό θα σημαίνει ότι το ελάχιστο μέγεθος καλύμματος κορυφών του G είναι το πολύ $|M|$. Από την άλλη μεριά όμως, εύκολα βλέπει κανείς (Άσκηση 6.16) ότι κάθε κάλυμμα κορυφών πρέπει να έχει τουλάχιστον $|M|$ κορυφές, οπότε η απόδειξη του Θεωρήματος 6.5 θα είναι πλήρης.

Επιλέγουμε λοιπόν να βάλουμε στο σύνολο U μια ακριβώς κορυφή από κάθε ακμή του M, και θα πρέπει να επιλέξουμε με κάποιο τρόπο ποια από τις δύο κορυφές να βάλουμε. Το κριτήριό μας θα είναι το παρακάτω:

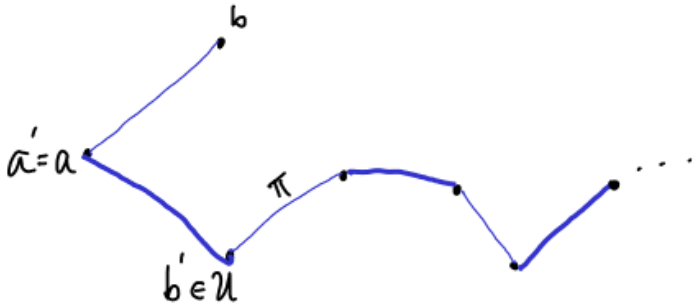
> Έστω $uv \in M$, με $u \in A, v \in B$. Αν υπάρχει εναλλακτικό μονοπάτι που καταλήγει στο v τότε βάζουμε την κορυφή v στο σύνολο U, αλλιώς βάζουμε την κορυφή u.

Είναι φανερό ότι με αυτή την κατασκευή ισχύει

$$|U| = |M|.$$

Απομένει να δείξουμε ότι το σύνολο U που κατασκευάσαμε είναι όντως κάλυμμα κορυφών του γραφήματος. Έστω λοιπόν ab μια ακμή του γραφήματος με $a \in A, b \in B$. Πρέπει να δείξουμε ότι τουλάχιστον ένα από τα a, b ανήκει στο U. Αν $ab \in M$ αυτό είναι προφανές οπότε υποθέτουμε ότι $ab \notin M$. Επειδή το M είναι μέγιστο ταίριασμα έπεται ότι υπάρχει $a'b' \in M$, με $a = a'$ ή $b = b'$, αλλιώς η ακμή $a'b'$ θα μπορούσε να προστεθεί στο M και το M να παραμείνει ταίριασμα, άρα αυτό δε μπορεί να ήταν μέγιστο ταίριασμα. Αν η a είναι αταίριαστη τότε $b = b'$ και η ακμή ab αποτελεί από μόνη της εναλλακτικό μονοπάτι, οπότε η κορυφή της $a'b'$ που επιλέχτηκε για το U ήταν η $b' = b$, και άρα πάλι δείξαμε αυτό που θέλουμε.

Μπορούμε συνεπώς να υποθέσουμε ότι $a = a'$. Αν το $a = a'$ δεν είναι στο U τότε $b' \in U$, άρα υπάρχει κάποιο εναλλακτικό μονοπάτι π που καταλήγει στο b'. (Δείτε την περίπτωση αυτή στο Σχήμα 6.7.)



Σχήμα 6.7: Μια περίπτωση στην απόδειξη του Θεωρήματος 6.5 (König–Egervary).

Οι βαριές ακμές είναι στο ταίριασμα M και οι άλλες όχι. Τότε όμως υπάρχει και κάποιο εναλλακτικό μονοπάτι π' που καταλήγει στο b: είτε το μέρος του π έως το b αν $b \in \pi$ είτε το $\pi' = \pi ab$ (το π ακολουθούμενο από το μονοπάτι $b'ab$). Επειδή το M είναι μέγιστο το π' πέρα από εναλλακτικό δε μπορεί να είναι και επαυξάνον μονοπάτι, άρα το b είναι ταιριασμένο στο M και είχε επιλεγεί για το U λόγω της ύπαρξης του εναλλακτικού μονοπατιού π' που καταλήγει στο b.

■

Παρατήρηση 6.6

Το Θεώρημα 6.5 μας δίνει τη δυνατότητα να **πιστοποιήσουμε** *ένα μέγιστο ταίριασμα. Φανταστείτε, για παράδειγμα, ότι έχετε μια εταιρεία που πουλάει μέγιστα ταιριάσματα σε διμερή γραφήματα. Έρχεται δηλ. ο πελάτης σας και σας δίνει ένα (τεράστιο) διμερές γράφημα, και ζητά από σας να βρείτε ένα μέγιστο*

ταίριασμα γι' αυτό. Για να σας πληρώσει όμως ζητάει και εγγυήσεις ότι το ταίριασμα που του βρήκατε είναι όντως μέγιστο. Τότε εσείς δεν έχετε παρά να του δώσετε, μαζί με το ταίριασμα M που υπολογίσατε, και ένα σύνολο κορυφών U, με τόσες κορυφές όσες το ταίριασμα έχει ακμές, και τέτοιο ώστε το U να είναι κάλυμμα όλων των ακμών του γραφήματος (κάθε ακμή του γραφήματος δηλ. να περιέχει κάποια κορυφή του U). Τέτοιο σύνολο κορυφών U υπάρχει λόγω του Θεωρήματος 6.4. Τότε, πάλι λόγω του Θεωρήματος 6.4, ο πελάτης σας (ο οποίος εύκολα μπορεί να επιβεβαιώσει τον ισχυρισμό σας ότι $|U| = |M|$ και ότι το U είναι κάλυμμα κορυφών) είναι βέβαιος ότι το M είναι μέγιστο ταίριασμα.

✏ **6.17**
Δίδεται ένας $m \times n$ πίνακας A με στοιχεία $A_{ij} \in \{0, 1\}$. Με **ευθεία** *του πίνακα εννούμε μια οποιαδήποτε γραμμή ή στήλη του. Δείξτε ότι το ελάχιστο πλήθος ευθειών που περιέχει όλα τα 1 του A είναι ίσο με το μέγιστο πλήθος από 1 που ανά δύο δε βρίσκονται πάνω στην ίδια ευθεία.*

💡 *Φτιάξτε ένα γράφημα G που έχει ως κορυφές όλες τις ευθείες του πίνακα A (το πλήθος τους είναι $m + n$) και ενώστε δύο ευθείες με μια ακμή αν και μόνο αν οι δύο αυτές ευθείες τέμνονται στον A και στην τομή τους υπάρχει άσος. Το γράφημα που δημιουργείται είναι φυσικά διμερές με τις δύο πλευρές να είναι οι γραμμές και οι στήλες του πίνακα. Ερμηνεύστε σε αυτό το γράφημα τις έννοιες «ταίριασμα» και «κάλυμμα» και εφαρμόστε το Θεώρημα 6.5.*

Παρατήρηση 6.7
Ας δείξουμε τώρα ότι το Θεώρημα 6.3 μπορεί να αποδειχθεί εύκολα χρησιμοποιώντας το Θεώρημα 6.5. Ουσιαστικά δίνουμε μια διαφορετική απόδειξη του Θεωρήματος του Γάμου η οποία χρησιμοποιεί το Θεώρημα König–Egerváry.

Πράγματι ας υποθέσουμε ότι σε ένα διμερές γράφημα ισχύει η συνθήκη (6.1) αλλά δεν υπάρχει πλήρες ταίριασμα του A. Από το Θεώρημα 6.5 υπάρχει σύνολο κορυφών U, με $|U| < |A|$, που είναι κάλυμμα κορυφών, έστω $U = A' \cup B'$ με $A' \subseteq A$ και $B' \subseteq B$. Έπεται ότι $|B'| < |A \setminus A'|$. Επειδή το U είναι κάλυμμα κορυφών έχουμε ότι δεν υπάρχουν στο G ακμές ανάμεσα στα σύνολα $A \setminus A'$ και $B \setminus B'$, άρα

$$\big|N(A \setminus A')\big| \leq \big|B'\big| < \big|A \setminus A'\big|,$$

και αυτό αντιφάσκει με την συνθήκη (6.1) για το σύνολο $J = A \setminus A'$.

6.4 Μονοπάτια και κυκλώματα Euler και Hamilton

6.4.1 Γενικά

Ορισμός 6.6
(Μονοπάτι Euler, Μονοπάτι Hamilton) *Μονοπάτι Euler (αντ. κύκλωμα Euler) ονομάζεται ένα μονοπάτι (αντ. κύκλωμα) που περνάει ακριβώς μία φορά από κάθε ακμή του γραφήματος.*

Μονοπάτι Hamilton (αντ. κύκλωμα Hamilton) ονομάζεται ένα μονοπάτι (αντ. κύκλωμα) που περνάει ακριβώς μία φορά από κάθε κορυφή του γραφήματος.

Δεν έχει κάθε γράφημα G κύκλωμα ή μονοπάτι Euler ή Hamilton. Εν γένει είναι πολύ δύσκολο να δώσει κανείς χρήσιμες αναγκαίες και ικανές συνθήκες για την ύπαρξη μονοπατιού ή κυκλώματος Hamilton. Επίσης από υπολογιστική άποψη η εύρεση μονοπατιού ή κυκλώματος Hamilton είναι ένα πολύ δύσκολο πρόβλημα. Ανήκει στην κλάση των λεγομένων NP-πλήρων (Nondeterministic Polynomial Time, NP) προβλημάτων για τα οποία πιστεύται ότι δεν επιδέχονται λύση σε πολυωνυμικό χρόνο. Για το συγκεκριμένο πρόβλημα, της ύπαρξης ή όχι μονοπατιού Hamilton σε ένα γράφημα G με n κορυφές πιστεύεται ισχυρά ότι δεν υπάρχει αλγόριθμος που, παίρνοντας σαν είσοδο το τυχόν γράφημα G, μας απαντάει ΝΑΙ αν το γράφημα έχει μονοπάτι Hamilton και ΟΧΙ αλλιώς, και, επιπλέον ο χρόνος που παίρνει (ο αριθμός των «βημάτων») είναι φραγμένος άνω από μια συνάρτηση της μορφής n^C όπου C είναι μια, ενδεχομένως μεγάλη, σταθερά (δεν εξαρτάται δηλ. από το n).

Αλλά, παρά τις ισχυρές ενδείξεις ότι αυτό συμβαίνει, αυτό δεν έχει αποδειχθεί ακόμη. Ενα άλλο αξιοσημείωτο που αφορά τα NP-πλήρη προβλήματα είναι ότι αυτά είναι αλληλένδετα με την εξής έννοια: αν ένα από αυτά δειχθεί ότι λύνεται σε πολυωνυμικό χρόνο, τότε όλα λύνονται. Αυτό βεβαίως

συνεπάγεται ότι και αν ένα από αυτά δειχθεί ότι δεν λύνεται σε πολυωνυμικό χρόνο τότε κανένα δε λύνεται. Επίσης, η κλάση αυτή προβλημάτων περιλαμβάνει εκατοντάδες προβλήματα τα οποία έχουν προκύψει πολύ φυσιολογικά.

6.4.2 Συνθήκες για κύκλωμα/μονοπάτι Euler

Η κατάσταση είναι τελείως διαφορετική για μονοπάτια και κυκλώματα Euler. Εχουμε το εξής απλό (και στη διατύπωση, και στην απόδειξη) θεώρημα.

Θεώρημα 6.6 *(α) Ενα συνεκτικό γράφημα G έχει κύκλωμα Euler αν και μόνο αν όλες οι κορυφές του G έχουν άρτιο βαθμό.*

(β) Ενα συνεκτικό γράφημα G έχει μονοπάτι Euler αν και μόνο αν όλες οι κορυφές του G έχουν άρτιο βαθμό ή όλες οι κορυφές του G εκτός από ακριβώς 2 έχουν άρτιο βαθμό.

Απόδειξη

Αποδεικνύουμε το (α).

Αν το G έχει κύκλωμα Euler

$$\pi : v_1 \longrightarrow \cdots \longrightarrow v_n = v_1,$$

τότε κάθε φορά που κάποια κορυφή v εμφανίζεται στο π «μπαίνουμε» στο v κινούμενοι πάνω στο π και μετά «<βγαίνουμε» από το v, χρησιμοποιώντας έτσι συνολικά 2 από τις ακμές που καταλήγουν στο v, οι οποίες δεν πρόκειται να ξαναχρησιμοποιηθούν, αφού το π περνάει από κάθε ακμή ακριβώς μια φορά. Με τον τρόπο αυτό (δηλ. σε ζεύγη πάντα) χρησιμοποιούνται όλες οι ακμές του v, άρα το v έχει άρτιο βαθμό.

Για το αντίστροφο, θα δείξουμε με επαγωγή ως προς τον αριθμό ακμών k ότι κάθε συνεκτικό γράφημα με k ακμές και όλες τις κορυφές με άρτιο βαθμό έχει κύκλωμα Euler.

Η μικρότερη τιμή του k με την οποία πρέπει να ασχοληθούμε είναι η τιμή $k = 3$, αφού δεν υπάρχει συνεκτικό γράφημα με λιγότερες από 3 ακμές και με όλες τις κορυφές να είναι άρτιου βαθμού. Το μόνο γράφημα που πληρεί τις προϋποθέσεις μας και έχει 3 ακμές είναι το τρίγωνο, το οποίο προφανώς και έχει κύκλωμα Euler.

Για την απόδειξη του επαγωγικού βήματος τώρα, υποθέτουμε ότι η πρόταση ισχύει για αριθμό ακμών $\leq k$ και έστω ότι έχουμε ένα γράφημα G με $k+1$ ακμές, συνεκτικό και με όλες τις κορυφές του να έχουν άρτιο βαθμό. Θα δείξουμε ότι έχει κύκλωμα Euler.

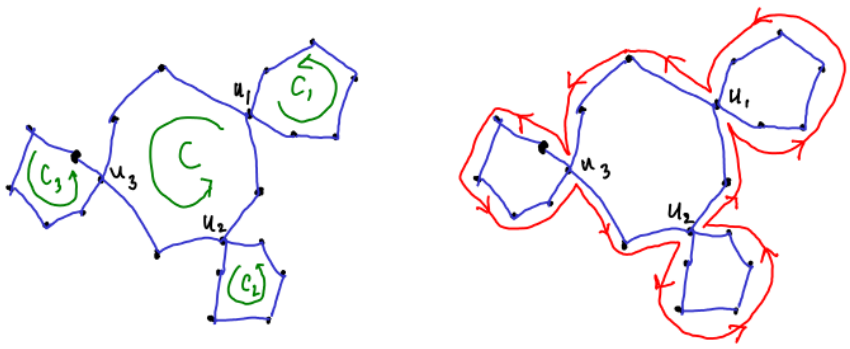
Αφού το G δεν έχει κορυφές περιττού βαθμού δε μπορεί να είναι δέντρο (κάθε δέντρο έχει φύλλα, δηλ. κορυφές βαθμού 1) άρα το G έχει κάποιο κύκλο, έστω C. Αν αφαιρέσουμε τον κύκλο αυτό από το γράφημα προκύπτει ένα νέο γράφημα G' του οποίου οι κορυφές εξακολουθούν να έχουν άρτιο βαθμό, αφού αφαιρώντας τον κύκλο από το γράφημα αφαιρούμε άρτιο πλήθος ακμών κάθε κορυφής. Αν το G' είναι κενό (δεν έχει ακμές) τότε έχουμε τελειώσει αφού ο κύκλος C περιέχει όλες τις ακμές του G και είναι συνεπώς κύκλωμα Euler. Ας υποθέσουμε από δω και πέρα ότι το G' δεν είναι το κενό γράφημα.

Το G' δεν είναι κατ' ανάγκη συνεκτικό. Ας είναι $G_1, G_2, \ldots, G_r$ οι συνεκτικές του συνιστώσες. Για κάθε ένα από το $G_1, G_2, \ldots, G_r$ ισχύουν οι υποθέσεις του Θεωρήματος (συνεκτικό, άρτιοι βαθμοί κορυφών) και κάθε ένα από αυτά έχει το πολύ k ακμές. Άρα, από την επαγωγική μας υπόθεση κάθε ένα από τα $G_1, G_2, \ldots, G_r$ έχει ένα κύκλωμα Euler, έστω C_i.

Παρατηρούμε τώρα ότι κάθε κύκλωμα C_i έχει κάποια κοινή κορυφή με τον κύκλο C. (Αν αυτό δε συνέβαινε το αρχικό μας γράφημα G θα ήταν ασύνδετο.) Ας είναι u_i μια κοινή κορυφή του C με το C_i. Ένα κύκλωμα Euler στο γράφημα G είναι τότε αυτό που προκύπτει αν διανύουμε τον κύκλο C και όποτε συναντήσουμε την κορυφή u_i αντί να συνεχίσουμε να διανύουμε τον κύκλο C παρεμβάλλουμε τον κύκλο C_i. Δείτε το Σχήμα 6.8.

Η απόδειξη του (β) είναι ανάγεται εύκολα στο (α) (δείτε την Άσκηση 6.18).

■



Σχήμα 6.8: Εδώ δείχνουμε πώς, στην απόδειξη του Θεωρήματος 6.6, ενώνουμε τα κυκλώματα C_i και C (πράσινο χρώμα) σε ένα μεγάλο κύκλωμα (κόκκινο χρώμα).

✏ **6.18**
Αποδείξτε το (β) του Θεωρήματος 6.6.
Προσθέστε έξυπνα μια ακμή και χρησιμοποιήστε το (α) του Θεωρήματος.

6.5 Χρωματισμοί

6.5.1 Γενικά

Ορισμός 6.7
Ενας χρωματισμός ενός συνόλου A με r χρώματα θα είναι μια συνάρτηση

$$\chi : A \to [r] = \{1, \ldots, r\}.$$

Αντί να αναφερόμαστε δηλ. στα χρώματα με άσπρο, κόκκινο, κλπ, τα αριθμούμε απλώς και προσδιορίζουμε το πόσα είναι.

Ορισμός 6.8
(Χρωματισμός κορυφών, χρωματισμός ακμών) *Εστω $G = (V, E)$ ένα γράφημα. Ενας χρωματισμός κορυφών του G με r χρώματα είναι μια συνάρτηση $\chi : V \to [r]$ τέτοια ώστε*

$$\forall u, v \in V : \ u \sim v \Longrightarrow \chi(u) \neq \chi(v).$$

Κορυφές που ενώνονται με ακμές δηλ. πρέπει να πάρουν αναγκαστικά διαφορετικό χρώμα.

Ομοίως χρωματισμός ακμών του G με r χρώματα είναι συνάρτηση $\chi : E \to [r]$ τ.ώ.

$$\forall e, e' \in E : \ \ e \sim e' \Longrightarrow \chi(e) \neq \chi(e').$$

Δηλ. ακμές που έχουν κοινή κορυφή πρέπει να πάρουν διαφορετικό χρώμα.

Προφανώς μπορούμε πάντα να χρωματίσουμε τις κορυφές ενός γραφήματος με n κορυφές χρησιμοποιώντας n χρώματα, ένα για κάθε κορυφή. Το ζητούμενο είναι αν μπορούμε να κάνουμε το ίδιο με λίγα χρώματα.

Ορισμός 6.9
(Χρωματικός αριθμός) *Ο χρωματικός αριθμός $\chi(G)$ ενός γραφήματος G είναι ο ελάχιστος φυσικός r για τον οποίο υπάρχει ένας χρωματισμός κορυφών του G.*

Παράδειγμα 6.7
Το πλήρες γράφημα με n κορυφές, K_n, χρειάζεται n χρώματα ($\chi(K_n) = n$), ενώ το κενό γράφημα χρειάζεται ένα μόνο ($\chi(E_n) = 1$).

✏ **6.19**
Δείξτε ότι ο κύκλος C_n έχει χρωματικό αριθμό $\chi(C_n) = 2$ αν n άρτιος και 3 αν n περιττός.

6.5.2 Εκτιμήσεις για τον χρωματικό αριθμό

Θα δώσουμε ένα άνω φράγμα για το $\chi(G)$ σε σχέση με το μέγιστο βαθμό των κορυφών του και ένα κάτω φράγμα σε σχέση με το πόσο μεγάλα πλήρη υπογραφήματα έχει. Αρχίζουμε με το κάτω φράγμα που είναι προφανές.

Θεώρημα 6.7
Αν το G έχει ένα υπογράφημα ισομορφικό με το K_s τότε $\chi(G) \geq s$.

Απόδειξη

Αν δηλ. το G έχει s κορυφές που όλες συνδέονται μεταξύ τους τότε χρειαζόμαστε τουλάχιστον s χρώματα για να χρωματίσουμε τις κορυφές του G, που είναι φανερό.
■

Το άνω φράγμα είναι πιο ενδιαφέρον.

Θεώρημα 6.8
Αν όλες οι κορυφές του G έχουν βαθμό $\leq d$ τότε $\chi(G) \leq d + 1$.

Απόδειξη

Με επαγωγή ως προς το πλήθος κορυφών n του G. Για $n = 1$ είναι φανερό.

Εστω G ένα γράφημα με n κορυφές και μέγιστο βαθμό d και έστω u οποιαδήποτε κορυφή του G. Ορίζουμε G' να είναι το υπογράφημα του G που προκύπτει αν διαγράψουμε την κορυφή u και όλες τις ακμές της. Αυτό έχει $n - 1$ κορυφές και μέγιστο βαθμό όχι μεγαλύτερο από πριν, άρα $\leq d$. Συνεπώς, από την επαγωγική μας υπόθεση, $\chi(G') \leq d + 1$, δηλ. μπορούμε να χρωματίσουμε τις κορυφές του G' με τα χρώματα $1, 2, \ldots, d + 1$.

Εστω τώρα οι γείτονες της u στο G', $u_1, \ldots, u_k$, με $k \leq d$. Αρα υπάρχει κάποιο από τα χρώματα $1, 2, \ldots, d + 1$ που δεν έχει χρησιμοποιηθεί στο χρωματισμό των $u_1, \ldots, u_k$, έστω το χρώμα c. Χρωματίζουμε τότε την κορυφή u με το χρώμα c και κρατάμε τα χρώματα των υπολοίπων κορυφών όπως στο χρωματισμό του G'. Εχουμε έτσι κατασκευάσει ένα χρωματισμό του G με $d + 1$ χρώματα.
■

✏ **6.20**
Αν $\chi(G) = k > 1$ δείξτε ότι το σύνολο κορυφών V του G μπορεί να διαμεριστεί σε δύο σύνολα $V = V_1 \cup V_2$ έτσι ώστε, αν G_i είναι το υπογράφημα του G που επάγεται από τις κορυφές V_i, $i = 1, 2$, τότε να ισχύει

$$\chi(G_1) + \chi(G_2) = k.$$

✏ **6.21**
Ας είναι G_1, G_2 δύο γραφήματα πάνω στο ίδιο σύνολο κορυφών V. Δείξτε ότι

$$\chi(G_1 \cup G_2) \leq \chi(G_1)\chi(G_2).$$

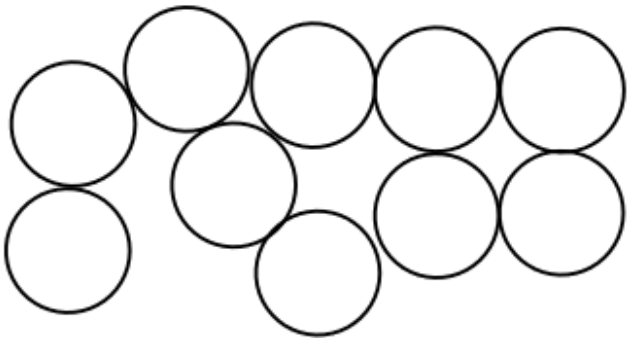
Εδώ με $G_1 \cup G_2$ συμβολίζουμε το γράφημα με σύνολο κορυφών V και με ακμές τις ακμές του G_1 μαζί με τις ακμές του G_2.

✏ **6.22**
Αν σε ένα γράφημα G με n κορυφές υπάρχουν s κορυφές που δε συνδέονται καθόλου μεταξύ τους δείξτε ότι

$$\chi(G) \leq n - s + 1.$$

✏ **6.23**

Στο επίπεδο εχουμε k ίσους κύκλους οι οποίοι δεν τέμνονται ανά δύο αλλά μπορούν να εφάπτονται (εξωτερικά, αφού είναι ίσοι). Δείξτε ότι μπορούμε να χρωματίσουμε τα εσωτερικά των κύκλων αυτών



Σχήμα 6.9: Κύκλοι στο επίπεδο όπως στην Άσκηση 6.23.

με το πολύ 4 διαφορετικά χρώματα με τρόπο τέτοιο ώστε αν δύο κύκλοι εφάπτονται τότε αυτοί να έχουν διαφορετικό χρώμα στο εσωτερικό τους.

Επαγωγή ως προς k. Εστιάσετε την προσοχή σας σε ένα κύκλο με ελάχιστη τετμημένη του κέντρου του.

Βιβλιογραφία Κεφαλαίου

[1] Peter J Cameron. *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, 1994.

[2] Reinhard Diestel. *Graph theory*. 2005.

[3] Chung Laung Liu and CL Liu. *Elements of discrete mathematics*. McGraw-Hill New York, 1985.

[4] Richard P Stanley. *Enumerative combinatorics*. 1986.

Κεφάλαιο 7

Τυπικές γλώσσες και αυτόματα

Κύρια βιβλιογραφική αναφορά για αυτό το Κεφάλαιο είναι η Hopcroft, Motwani, and Ullman 2007.

7.1 Αλφάβητα, λέξεις και γλώσσες

Ορισμός 7.1
(Αλφάβητο) Αλφάβητο *είναι ένα οποιοδήποτε μη κενό πεπερασμένο σύνολο, του οποίου τα στοιχεία ονομάζουμε* σύμβολα *ή* γράμματα .

Παράδειγμα 7.1
Το δυαδικό αλφάβητο $\Sigma_2 = \{0, 1\}$. *Υπό μία έννοια αυτό είναι το πλέον ενδιαφέρον αλφάβητο. Ένας λόγος είναι ότι αυτό είναι το αλφάβητο που χρησιμοποιείται στους σημερινούς υπολογιστές. Ο σημαντικότερος όμως λόγος είναι ότι το Σ_2 μπορεί να «μιμηθεί» αποτελεσματικά οποιοδήποτε άλλο αλφάβητο. Το τι σημαίνει αυτό ελπίζουμε να γίνει ξεκάθαρο αργότερα.*

Παράδειγμα 7.2
Το αλφάβητο $\Sigma_{GR} = \{A, B, \Gamma, \ldots, \alpha, \beta, \gamma, \ldots, \omega, \ldots\}$ περιλαμβάνει όλα τα γράμματα και σημεία στίξης της Ελληνικής γλώσσας.

Ορισμός 7.2
(Λέξη) Λέξη *πάνω από ένα αλφάβητο Σ λέγεται μια πεπερασμένη ακολουθία*

$$\alpha = \alpha_1 \ldots \alpha_n$$

γραμμάτων $\alpha_i \in \Sigma$, ενδεχομένως και κενή (δηλ. με $n = 0$).
Ο αριθμός $n \geq 0$ λέγεται μήκος *της λέξης α και συμβολίζεται με $|\alpha|$.*
Η κενή λέξη συμβολίζεται πάντα με το ϵ.
Με Σ^* συμβολίζουμε το σύνολο όλων των λέξεων πάνω από το αλφάβητο Σ.

Παράδειγμα 7.3
Η $w = 0101$ είναι μια λέξη πάνω από το δυαδικό αλφάβητο Σ_2, με μήκος $|w| = 4$.

Ορισμός 7.3
(Γλώσσα) *Μια γλώσσα L πάνω από ένα αλφάβητο Σ είναι ένα οποιοδήποτε σύνολο, πεπερασμένο ή άπειρο, λέξεων πάνω από το Σ. Ως συνήθως στα μαθηματικά με $|L|$ συμβολίζουμε τον πληθάριθμο της L.*

Παράδειγμα 7.4
Το κενό σύνολο $\emptyset$ αποτελεί μια γλώσσα πάνω από οποιοδήποτε αλφάβητο Σ που θα το ονομάζουμε κενή γλώσσα .

Παράδειγμα 7.5
Αν είναι Σ ένα αλφάβητο τότε, καταχρηστικά, συμβολίζουμε πάλι με Σ τη γλώσσα πάνω από το Σ που αποτελείται από όλες τις δυνατές λέξεις με ακριβώς ένα γράμμα, το ίδιο δηλ. το αλφάβητο με μία έννοια.

Παράδειγμα 7.6
Το σύνολο Σ^* όλων των λέξεων πάνω από ένα αλφάβητο Σ είναι η πλήρης *γλώσσα πάνω από το Σ. Για οποιοδήποτε Σ αυτή είναι μια άπειρη γλώσσα που περιέχει ως υπογλώσσες (υποσύνολα) όλες τις γλώσσες πάνω από το Σ.*

Παράδειγμα 7.7
Το σύνολο E όλων των επωνύμων που εμφανίζονται τον τηλεφωνικό κατάλογο Κρήτης του 2015 αποτελεί μια γλώσσα πάνω από το αλφάβητο Σ_{GR} των γραμμάτων και σημείων στίξης της ελληνικής γλώσσας (υποθέτουμε εδώ ότι δεν χρησιμοποιούνται πουθενά γράμματα του λατινικού αλφαβήτου στον κατάλογο). Η E είναι μια πεπερασμένη αλλά μεγάλη γλώσσα.

Παράδειγμα 7.8
Το σύνολο

$$Q = \left\{ w \in \Sigma_2^* : \exists k \in \mathbb{N} : \ |w| = k^2 \right\}$$

είναι η γλώσσα όλων των δυαδικών λέξεων με μήκος που είναι τέλειο τετράγωνο. Προφανώς πρόκειται για μια άπειρη γλώσσα.

Παράδειγμα 7.9
Το σύνολο L_k όλων των λέξεων του Σ_2 με μήκος ακριβώς k, όπου k είναι ένας φυσικός αριθμός, είναι μια πεπερασμένη υπογλώσσα του Σ_2^*. Για διαφορετικά k, k' οι δύο γλώσσες $L_k, L_{k'}$ είναι ξένες μεταξύ τους. Για κάθε λέξη $w \in \Sigma_2^*$ υπάρχει ακριβώς ένα k, το $k = |w|$, για το οποίο $w \in L_k$. Οι γλώσσες L_k, $k \geq 0$, αποτελούν συνεπώς μια διαμέριση της πλήρους γλώσσας Σ_2^*.

✏ **7.1**

Το παρακάτω πρόγραμμα σε python τυπώνει όλες τις λέξεις με δεδομένο μήκος πάνω από ένα δοσμένο αλφάβητο.

```
def words_of_length(S, k):
    """ Return a list with all words over alphabet S of length k"""
    if k==0:
        return ['']
    result = []
    tails = words_of_length(S, k-1)
    for first in S:
        for t in tails:
            result.append(first+t)
    return result

S = ['a', 'b']
print words_of_length(S, 3)
SS = ['a', 'b', 'c']
print words_of_length(SS, 3)
print words_of_length(SS, 0)
```

Το αποτέλεσμα αυτού του προγράμματος είναι:

```
['aaa', 'aab', 'aba', 'abb', 'baa', 'bab', 'bba', 'bbb']
['aaa', 'aab', 'aac', 'aba', 'abb', 'abc', 'aca', 'acb', 'acc', 'baa',
 'bab', 'bac', 'bba', 'bbb', 'bbc', 'bca', 'bcb', 'bcc', 'caa', 'cab',
 'cac', 'cba', 'cbb', 'cbc', 'cca', 'ccb', 'ccc']
['']
```

Βεβαιωθείτε ότι καταλαβαίνετε πώς δουλεύει και πειραματιστείτε με αυτό ορίζοντας μερικά δικά σας αλφάβητα. Τροποποιήστε το ώστε να τυπώνει όλες τις λέξεις μήκους μέχρι k.

✏ **7.2**

Βρείτε το $|L_k|$. Αν M_k είναι η υπογλώσσα του Σ_2^* που αποτελείται από όλες τις λέξεις με μήκος το πολύ k, βρείτε το $|M_k|$.

✏ **7.3**
Πόσες λέξεις μήκους n υπάρχουν πάνω από ένα αλφάβητο με k γράμματα;

Παράδειγμα 7.10
Ας είναι Σ_A το αλφάβητο που αποτελείται από τα γράμματα του λατινικού αλφαβήτου, μικρά και κεφαλαία, τα δεκαδικά ψηφία, σημεία στίξης, παρενθέσεις, αγκύλες, τον λευκό *(space) χαρακτήρα (να μη συγχέεται με την κενή λέξη ϵ), το χαρακτήρα αλλαγής γραμμής (carriage return), και γενικά όλα τα σύμβολα που εμφανίζονται σε ένα σύγχρονο πληκτρολόγιο υπολογιστή. Αυτό το αλφάβητο ονομάζεται και αλφάβητο American Standard Code For Information Interchange – ASCII. (Για την ακρίβεια ο* κώδικας *ASCII είναι ένα standard αντιστοίχισης όλων των συμβόλων που αναφέραμε παραπάνω στους αριθμούς 0-127. Το standard αυτό ακολουθείται σήμερα σε όλους τους υπολογιστές.)*

Η γλώσσα L_C είναι εκείνο το σύνολο από λέξεις του Σ_A^* που αποτελούν συντακτικά σωστά προγράμματα στη γλώσσα προγραμματισμού python. Αν δεν είστε γνώστες της γλώσσας αυτής αλλά κάποιας άλλης, μπορείτε να ορίσετε την αντίστοιχη γλώσσα. Ένα πρόγραμμα λοιπόν δεν είναι τίποτε άλλο από μια λέξη σε ένα κατάλληλο αλφάβητο. Αν αυτό ξενίζει να θυμίσουμε ότι και οι χαρακτήρες αλλαγής γραμμής βρίσκονται μέσα στο αλφάβητο, και άρα μια λέξη του L_C μπορεί να περιέχει τα γράμματα ενός ολόκληρου αρχείου κειμένου.

Το L_C είναι μια άπειρη γλώσσα αφού δεν υπάρχει άνω όριο στο μέγεθος ενός συντακτικά σωστού προγράμματος, και άρα υπάρχουν άπειρα τέτοια.

Ορισμός 7.4
(Συγκόλληση λέξεων, πρόθεμα και επίθεμα λέξης) *Αν $\alpha = \alpha_1 \dots \alpha_m$ και $\beta = \beta_1 \dots \beta_n$ είναι δύο λέξεις πάνω από το αλφάβητο Σ με μήκη m και n, τότε ορίζουμε τη* συγκόλληση *(concatenation) $\alpha\beta$ να είναι η λέξη*

$$\alpha\beta = \alpha_1 \dots \alpha_m \beta_1 \dots \beta_n,$$

που έχει μήκος το άθροισμα των μηκών.

Μια λέξη π λέγεται πρόθεμα *(prefix) μιας λέξης α αν υπάρχει λέξη β τ.ώ. $\alpha = \pi\beta$. Ομοίως η π λέγεται* επίθεμα *(suffix) της α αν υπάρχει β τ.ώ. $\alpha = \beta\pi$.*

Τέλος, μια λέξη π λέγεται υπολέξη της w αν υπάρχουν λέξεις α, και β, ενδεχομένως κενές, τέτοιες ώστε $w = \alpha\pi\beta$.

Παράδειγμα 7.11
Αν $\Sigma = \{a, b, c\}$ τότε η συγκόλληση των λέξεων abc και bb είναι η λέξη $abcbb$.

Παράδειγμα 7.12
Τα προθέματα της λέξης $abcd$ (δεν έχει σημασία σε ποιο αλφάβητο δουλεύουμε) είναι οι λέξεις $\epsilon, a, ab, abc, abcd$. Τα επιθέματα είναι οι λέξεις $abcd, bcd, cd, d, \epsilon$.

Παρατήρηση 7.1
Προφανώς ισχύει πάντα $\alpha\epsilon = \epsilon\alpha = \alpha$, για κάθε λέξη α.

Είναι φανερό ότι μια λέξη με μήκος n έχει ακριβώς $n + 1$ προθέματα και άλλα τόσα επιθέματα.

Επίσης η συγκόλληση λέξεων είναι μια πράξη μη αντιμεταθετική, αφού, για παράδειγμα, αν $\alpha = 01$ και $\beta = 00$ τότε $\alpha\beta = 0100 \neq 0001 = \beta\alpha$.

Παρατήρηση 7.2
Αν τ είναι γράμμα ενός αλφαβήτου Σ τότε συμβολίζουμε επίσης με τ τη γλώσσα πάνω από το Σ που περιέχει μόνο μια λέξη, τη λέξη τ, που έχει μόνο ένα γράμμα.

Ορισμός 7.5
(Συγκόλληση γλωσσών) *Αν L_1, L_2 είναι δύο γλώσσες πάνω από το Σ ορίζουμε τη συγκόλληση L_1L_2 αυτών να είναι η γλώσσα*

$$L_1L_2 = \{xy : \ x \in L_1, y \in L_2\}.$$

Αποτελείται δηλ. η L_1L_2 από όλες τις λέξεις που προκύπτουν ως συγκόλληση μιας λέξης από την L_1 με μια λέξη της L_2.

Ορίζουμε επίσης $L^0 = \{\epsilon\}$ *και, για* $n \geq 1$, $L^n = LL\cdots L$ *(συγκόλληση της* L *με τον εαυτό της* n *φορές).*

Τέλος ορίζουμε

$$L^* = \bigcup_{k=0}^{\infty} L^k$$

και

$$L^+ = \bigcup_{k=1}^{\infty} L^k.$$

Παράδειγμα 7.13
Έστω $L = \{00, 11, \epsilon\}$. *Τότε* $L^* = L^+$ *είναι η γλώσσα που απαρτίζεται από όλες εκείνες τις λέξεις από 0 ή 1 με άρτιο μήκος όπου το πρώτο γράμμα είναι ίδιο με το δεύτερο, το τρίτο με το τέταρτο κλπ. Η κενή λέξη ανήκει στην* L^*.

✏ **7.4**
Περιγράψτε τη γλώσσα 1^* *πάνω από το δυαδικό αλφάβητο* Σ_2.

✏ **7.5**
Δείξτε ότι για κάθε γλώσσα L *και φυσικούς αριθμούς* m, n *ισχύει* $L^{m+n} = L^m L^n$.

✏ **7.6**
Αν L *είναι μια οποιαδήποτε γλώσσα που δεν περιέχει την κενή λέξη* ϵ, *ποια είναι ακριβώς η διαφορά των γλωσσών* L^* *και* L^+; *Αλλάζει κάτι στην απάντηση αν* $\epsilon \in L$;

✏ **7.7**
Βεβαιωθείτε ότι καταλαβαίνετε τι περιγράφει η γλώσσα

$$\{+, -, \epsilon\}1\{0, 1\}^*.$$

(Πρόκειται για συγκόλληση τριών γλωσσών.) Όταν, όπως εδώ, δεν περιγράφουμε το αλφάβητο, αυτό συνάγεται από όλα τα σύμβολα που έχουν χρησιμοποιηθεί, στην προκειμένη περίπτωση δηλαδή $\Sigma = \{0, 1, +, -\}$.

7.2 Ντετερμινιστικά Αυτόματα

Ένα Ντετερμινιστικό Αυτόματο (Deterministic Finite Automaton ή DFA) είναι ουσιαστικά ένα κατευθυνόμενο γράφημα, του οποίου οι κορυφές Q ονομάζονται *καταστάσεις* (states) και από κάθε κορυφή φεύγει ακριβώς μια ακμή για κάθε γράμμα του αλφαβήτου Σ. Υπάρχει μια διακεκριμένη κατάσταση q_0, η *αρχική κατάσταση* και ένα μη-κενό σύνολο F από *τελικές καταστάσεις*.

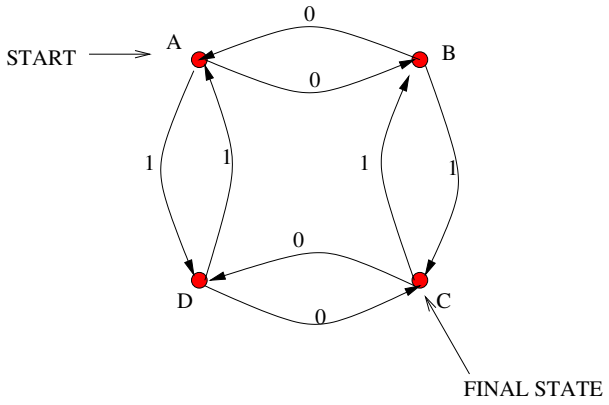
Δείτε π.χ. ένα τέτοιο αυτόματο στο Σχήμα 7.1.

Ορισμός 7.6
(Ντετερμινιστικό Αυτόματο)
Ένα ντετερμινιστικό αυτόματο *είναι μια πεντάδα*

$$(Q, \Sigma, \delta, q_0, F)$$

όπου

- Q *είναι ένα πεπερασμένο σύνολο* καταστάσεων,
- Σ *είναι ένα πεπερασμένο αλφάβητο,*



Σχήμα 7.1: Ένα απλό ντετερμινιστικό αυτόματο

- δ *είναι η* συνάρτηση μετάβασης *(transition function) με πεδίο ορισμού το* $Q \times \Sigma$ *και πεδίο τιμών το* Q*,*
- $q_0 \in Q$ *είναι μια από τις καταστάσεις που ονομάζεται* αρχική*, και*
- $F \subseteq Q$ *είναι το σύνολο των* τελικών *καταστάσεων.*

Παρατήρηση 7.3
Ένα DFA το σχεδιάζουμε συνήθως ως ένα κατευθυνόμενο γράφημα με σύνολο κορυφών ίδιο με το σύνολο καταστάσεων Q*. Από κάθε κατάσταση/κορυφή* q *φεύγει ακριβώς μια ακμή για κάθε γράμμα* $a \in \Sigma$ *η οποία καταλήγει στην κατάσταση* $\delta(q, a)$*.*

Παράδειγμα 7.14
Στο αυτόματο που φαίνεται στο Σχήμα 7.1 έχουμε $Q = \{A, B, C, D\}$*,* $\Sigma = \{0, 1\}$*,* $q_0 = A$*,* $F = \{C\}$*.*

Για να μιλήσουμε για τη συνάρτηση μετάβασης δ θα πρέπει πρώτα να αναφερθούμε στον τρόπο «λειτουργίας » του αυτομάτου. Ένα αυτόματο χρησιμεύει για να *αναγνωρίζει*, όπως λέμε, μια γλώσσα $L \subseteq \Sigma^*$. Η διαδικασία αναγνώρισης είναι η εξής.

Έστω λέξη $w \in \Sigma^*$, $w = w_1 \dots w_n$, μήκους n ($w_i \in \Sigma$).

- Το αυτόματο αρχίζει τη λειτουργία του στην αρχική κατάσταση q_0.
- Διαβάζει έπειτα τα γράμματα της λέξης ένα προς ένα, από τα αριστερά προς τα δεξιά πάντα. Πρώτο διαβάζεται το γράμμα w_1 και τελευταίο το w_n.
- Μόλις διαβάσει το γράμμα $\alpha \in \Sigma$ και ευρισκόμενο στην κατάσταση q το αυτόματο *μεταβαίνει* στην κατάσταση r αν και μόνο αν η ακμή $q \to r$ έχει ετικέτα (label) ίση με α. Για κάθε κατάσταση του αυτομάτου και κάθε γράμμα του αλφαβήτου υπάρχει εξ ορισμού ακριβώς μια ακμή που ξεκινά από την κατάσταση αυτή και έχει ετικέτα αυτό το γράμμα. Ισχύει τότε για τη συνάρτηση μετάβασης $\delta(q, \alpha) = r$, χρησιμεύει δηλ. η συνάρτηση μετάβασης για να μας προσδιορίσει σε ποια κατάσταση πάει το αυτόματο αν βρίσκεται σε μια δεδομένη κατάσταση q και διαβάσει ένα συγκεκριμένο γράμμα α. Όλη η συνδεσμολογία του αυτομάτου δηλ. είναι κωδικοποιημένη στη συνάρτηση δ.
- Αφού διαβάσει το αυτόματο το τελευταίο γράμμα της λέξης και κάνει την τελευταία του μετάβαση δηλώνει ότι αποδέχεται τη λέξη αν και μόνο αν βρίσκεται σε τελική κατάσταση, σε μια κατάσταση δηλ. του συνόλου F. Αλλιώς η λέξη απορρίπτεται.

Ορισμός 7.7
(Γλώσσα ενός DFA)
Το σύνολο των λέξεων που αποδέχεται το αυτόματο M ονομάζεται η γλώσσα που αναγνωρίζει το αυτόματο *και συμβολίζεται με $L(M)$.*

Παράδειγμα 7.15
Ποια είναι η γλώσσα L που αναγνωρίζεται από το αυτόματο της εικόνας 7.1;

Δε θέλει και πολλή σκέψη για να πειστούμε ότι στην L ανήκουν ακριβώς εκείνες οι λέξεις του $\{0,1\}^*$ που έχουν περιττό αριθμό από 0 και περιττό αριθμό από 1. Για να το δούμε αυτό παρατηρούμε ότι οποτεδήποτε το αυτόματο βρίσκεται σε μια από τις δύο αριστερές καταστάσεις το πλήθος των μηδενικών που έχει διαβάσει είναι άρτιο. Αυτό γίνεται γιατί αυτή η πρόταση ισχύει προφανέστατα τη χρονική στιγμή 0, αφού τότε δεν έχει διαβάσει κανένα μηδενικό και βρίσκεται στην αρχική κατάσταση A που είναι στην αριστερή μεριά. Οποτεδήποτε διαβάσει επίσης κάποιο μηδενικό το αυτόματο αλλάζει μεριά και διατηρείται έτσι η ιδιότητα αυτή. Ομοίως επιχειρηματολογώντας βλέπουμε ότι το αυτόματο βρίσκεται σε μια από τις δύο πάνω καταστάσεις (A και B) αν και μόνο αν έχει διαβάσει άρτιο αριθμό από 1. Έτσι, το να είναι το αυτόματο στην κατάσταση C (τελική) σημαίνει ότι έχει δει περιττό αριθμό από ένα και περιττό από μηδέν, αφού η C είναι κάτω (περιττοί άσοι) και δεξιά (περιττά μηδενικά).

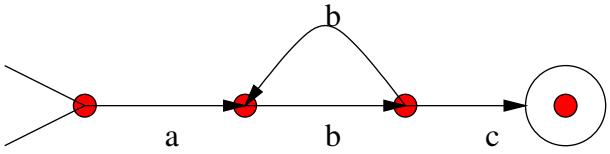
Αν π.χ. θελήσουμε να έχουμε ένα αυτόματο που θα αναγνωρίζει ακριβώς εκείνες τις λέξεις του $\{0,1\}^*$ που έχουν περιττά μηδενικά ή άρτιους άσους *η μόνη αλλαγή που χρειάζεται να κάνουμε στην περιγραφή του αυτομάτου είναι να αλλάξουμε το σύνολο F των τελικών καταστάσεων και να το θέσουμε ίσο με το $\{A, B, C\}$.*

✏ **7.8**
Σχεδιάστε ένα DFA που να αναγνωρίζει εκείνες τις λέξεις πάνω από το $\Sigma = \{0,1\}$ που έχουν άρτιο πλήθος άσων και πλήθος μηδενικών που είναι πολλαπλάσιο του 3.
Δείτε το Σχήμα 7.2.

Σχήμα 7.2: Για την Άσκηση 7.8 δουλέψτε με 6 καταστάσεις όπως αυτές.

✏ **7.9**
Σχεδιάστε ένα DFA που αναγνωρίζει εκείνες τις λέξεις πάνω από το $\Sigma = \{0,1\}$ που αρχίζουν από 11011.

Παράδειγμα 7.16
Στο σχήμα 7.3 βλέπουμε ένα αυτόματο που αναγνωρζει τη γλώσσα $a\{bb\}^*bc$, δηλ. όλες εκείνες τις λέξεις στο αλφάβητο $\Sigma = \{a, b\}$ που αρχίζουν με a, ακολουθεί ένας οποιοσδήποτε αριθμός (ακόμη και μηδέν) από αντίγραφα της λέξης bb, και τελειώνουν με τη λέξη bc.



Σχήμα 7.3: DFA για τη γλώσσα $a\{bb\}^*bc$

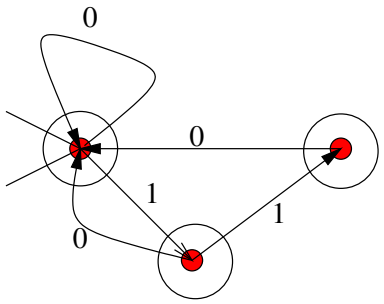
Συμβολισμός: Στο Σχήμα 7.3, όπως και παρακάτω, συμβολίζουμε την αρχική κατάσταση με μια ανοιχτή γωνία (σα «χωνί», απ' όπου μπαίνουμε στο αυτόματο) και κάθε τελική κατάσταση μπαίνει μέσα σ'ένα κύκλο.

Συμβολισμός: Προσέξτε ότι στο αυτόματο του Σχήματος 7.3 δεν ισχύει η αρχική μας απαίτηση ότι από κάθε κορυφή πρέπει να φεύγει ακριβώς μια ακμή για κάθε γράμμα του αλφαβήτου (ώστε ό,τι και να διαβάσουμε όταν είμαστε σε κάποια κατάσταση να έχουμε που να πάμε). Για παράδειγμα, για τη δεύτερη κορυφή από αριστερά δεν υπάρχει ακμή με ετικέτα a που να ξεκινάει από αυτή. Η σύμβαση που ακολουθούμε είναι ότι αν διαβάσουμε ένα σύμβολο και βρισκόμαστε σε μια κατάσταση από την οποία δεν ξεκινάει ακμή με ετικέτα αυτό το σύμβολο, τότε η λέξη *δεν αναγνωρίζεται* από το αυτόματο.

Η σύμβαση αυτή ακολουθείται καθαρά για λόγους αισθητικής και κατανόησης του σχεδίου και δεν αλλάζει απολύτως τίποτα στην ουσία. Κάθε αυτόματο που ακολουθεί τη σύμβαση αυτή μπορεί εύκολα να μετατραπεί σε ένα αυτόματο που δε χρησιμοποιεί αυτή τη σύμβαση και έχει πράγματι μια ακμή για κάθε γράμμα από κάθε κορυφή. Απλά δηλώνουμε μια νέα *μη τελική* κατάσταση K, την κατάσταση καταστροφής, όπως επιλέγουμε να την ονομάσουμε, και από κάθε άλλη κατάσταση του αυτομάτου που δεν έχει ακμή από αυτή με ετικέτα έστω x ορίζουμε μια τέτοια ακμή προς την K. Όλες οι ακμές από το K επιστρέφουν πάλι στο K. Είναι εύκολο να δούμε ότι οι ίδιες ακριβώς λέξεις αναγνωρίζονται από το αρχικό και το νέο αυτόματο.

Παράδειγμα 7.17

Ακολουθεί στο Σχήμα 7.4 ένα αυτόματο που αναγνωρίζει τη γλώσσα L εκείνων των λέξεων του $\{0,1\}^*$ που έχουν μέσα το πολύ δύο διαδοχικά 1. Ισοδύναμα, είναι εκείνες οι λέξεις στις οποίες δεν εμφανίζεται *η μορφή 111.*



Σχήμα 7.4: DFA για τις λέξεις χωρίς τρία διαδοχικά 1

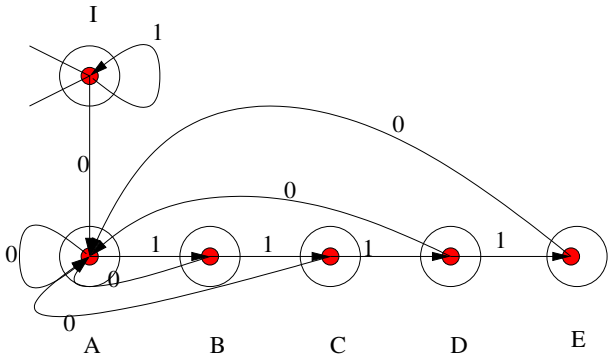
Στο αυτόματο αυτό όλες οι καταστάσεις είναι τελικές, αλλά αυτό δεν αποτελεί αντίφαση, αφού ακολουθούμε τη σύμβαση της άνω παρατήρησης. Έτσι υπάρχουν πράγματι λέξεις που δεν αναγνωρίζονται από το αυτόματο, μια και κάποιες κορυφές δεν έχουν ακμές που ξεκινάνε από αυτές και για το 0 και το 1. Η μόνη τέτοια κορυφή είναι η δεξιά, και, όντως, η μόνη περίπτωση να απορριφθεί μια λέξη από το αυτόματο είναι να είμαστε στη δεξιά κατάσταση και να διαβάσουμε 1, πράγμα το οποίο συμβαίνει αν και μόνο αν υπάρχουν τρία διαδοχικά 1 στη λέξη.

Παράδειγμα 7.18

Το παράδειγμα αυτό είναι κάπως πιο ενδιαφέρον: L είναι η γλώσσα εκείνων των λέξεων του $\{0,1\}^*$ που είναι τέτοιες ώστε, μετά το πρώτο 0 *υπάρχει τουλάχιστον ένα 0 σε κάθε πεντάδα διαδοχικών γραμμάτων της λέξης. Για παράδειγμα, οι λέξεις 11111111111, 11111110111101111 είναι στην L ενώ η λέξη 111111011111 δεν είναι (η τελευταία πεντάδα δεν έχει 0). Το αυτόματο δίνεται στο Σχήμα 7.5.*

Πώς πρέπει να σκεφθεί κανείς για να καταλάβει πώς δουλεύει το συγκεκριμένο αυτόματο;

Το κλειδί σε αυτή την περίπτωση, όπως και στις περισσότερες, είναι να αποδώσουμε κάποιο νόημα στην πρόταση «βρισκόμαστε στην τάδε κατάσταση». Για παράδειγμα, στην κατάσταση I βρισκόμαστε ακριβώς όταν δεν έχουμε διαβάσει ακόμη το πρώτο 0 της λέξης. Η πρόταση αυτή ισχύει κατ' αρχήν (πριν έχουμε διαβάσει τίποτε) και διατηρείται από οποιαδήποτε μετάβαση, αφού φεύγουμε από την κατάσταση I ακριβώς



Σχήμα 7.5: DFA για τις λέξεις με τουλάχιστον ένα 0 σε κάθε πεντάδα, μετά το πρώτο 0

μόλις διαβάσουμε το πρώτο μηδενικό και δεν ξαναγυρνάμε σε αυτή. Είναι τώρα φανερό, έχοντας ξεκαθαρίσει τι σημαίνει να βρισκόμαστε στην κατάσταση I, ότι αυτή πρέπει να είναι τελική κατάσταση, μια και αν ποτέ δε διαβάσουμε κάποιο 0, ισχύει ο κανόνας που βάλαμε στην αρχή για το ποιες λέξεις ανήκουν στην L και άρα πρέπει να δεχτούμε τη λέξη.

Κάνουμε τώρα την εξής παρατήρηση. Ας πούμε πως ένας άνθρωπος, με λίγη μνήμη, έχει επιφορτισθεί με το καθήκον να αναγνωρίζει ακριβώς αυτές τις λέξεις. Αυτός μαθαίνει τα σύμβολα της λέξης ένα-ένα, πρώτα από τα αριστερά, όπως ακριβώς και το αυτόματο, και πρέπει κάποια στιγμή να πεί αν αυτή η λέξη ανήκει ή όχι στην L. Επειδή ακριβώς ο άνθρωπος αυτός έχει λίγη μνήμη, κι επειδή οι λέξεις τις οποίες κρίνει μπορούν να έχουν οσοδήποτε μεγάλο μήκος, αποφασίζει αντί ανά πάσα στιγμή να θυμάται ολόκληρη τη λέξη που έχει δει μέχρι τότε, να θυμάται απλώς πόσο χρόνο πριν είδε το τελευταίο μηδενικό. *Είναι φανερό ότι αυτή η πληροφορία του αρκεί για να αποφασίσει. Θα απορρίψει δε τη λέξη αν και μόνο αν αυτός ο χρόνος ξεπεράσει το 5 σε κάποια χρονική στιγμή, γιατί ακριβώς τότε έχει δει μια πεντάδα γεμάτη με 1.*

Μετά από αυτή την παρατήρηση το νόημα της κατάστασης A είναι ότι βρίσκεται εκεί αν έχει δεί 0 ακριβώς πριν από χρόνο 1. Το νόημα της κατάστασης B ομοίως είναι ότι έχει δεί το τελευταίο 0 ακριβώς πριν από χρόνο 2, κ.ο.κ., ενώ στην κατάσταση E βρισκόμαστε αν έχουμε δεί το τελευταίο 0 ακριβώς 5 χρονικές στιγμές πριν. Είναι φανερό τώρα γιατί η κατάσταση E δεν έχει μετάβαση που ξεκινά από αυτή με 1: αν είδαμε το τελευταίο 0 χρόνο 5 πίσω και μας έρθει 1 πάει να πει πως έχουμε μόλις συμπληρώσει μια πεντάδα γεμάτη με 1. Άρα δεν υπάρχει λόγος να συνεχίσουμε γιατί, ό,τι και να δούμε από δω και πέρα, η λέξη πρέπει να απορριφθεί.

Εύκολα μπορούμε τώρα να ελέγξουμε ότι οι διάφορες μεταβάσεις στο σχήμα 7.5 είναι φτιαγμένες ακριβώς ώστε ακολουθώντας αυτές να διατηρείται το νόημα της κάθε κατάστασης, και άρα το αυτόματο δουλεύει. Αν, για παράδειγμα, βρισκόμαστε σε μια οποιαδήποτε από τις καταστάσεις $A, \ldots, E$ και διαβάσουμε 0 πρέπει να μεταβούμε στην κατάσταση A αφού μετά τη μετάβασή μας θα έχουμε διαβάσει 0 ακριβώς χρόνο 1 πριν, και αυτό είναι το νόημα της κατάστασης A.

✏ **7.10**

Κατασκευάστε ένα DFA που αναγνωρίζει εκείνες τις λέξεις πάνω από το $\Sigma = \{0, 1\}$ που έχουν μήκος τουλάχιστον 5 και το 5ο γράμμα τους από τα αριστερά είναι 1.

✏ **7.11**

Κατασκευάστε ένα DFA που αναγνωρίζει εκείνες τις λέξεις πάνω από το $\Sigma = \{0, 1\}$ που έχουν μήκος τουλάχιστον 5 και το 5ο γράμμα τους από τα δεξιά είναι 1.

✏ **7.12**

L είναι η γλώσσα εκείνων των λέξεων του $\{0, 1\}^*$ που είναι τέτοιες ώστε, μετά το πρώτο 0 *υπάρχουν τουλάχιστον δύο 0 σε κάθε πεντάδα διαδοχικών γραμμάτων της λέξης. Κατασκευάστε ένα DFA που αναγνωρίζει την L.*

✏ **7.13**
Κατασκευάστε DFA για τις γλώσσες του $\{0,1\}^*$*:*

1. *Λέξεις που τελειώνουν σε 00*
2. *Λέξεις που περιέχουν τρία διαδοχικά 0*

✏ **7.14**
Κατασκευάστε DFA για τις γλώσσες

(α) 00^*1^*1*, και*

(β) $\{w \in \{a,b\}^* : \ 6 \mid A(w) + 2B(w)\}$*,*

όπου $A(w)$*, και* $B(w)$ *είναι το πλήθος των* a *και των* b *στη λέξη* w *και* $x|y$ *σημαίνει ότι το* x *διαιρεί το* y*.*

✏ **7.15**
Αν M *είναι DFA δείξτε πώς να κατασκευάσετε ένα DFA για τη γλώσσα* $\Sigma^* \setminus L(M)$ *(το συμπλήρωμα της γλώσσας* $L(M)$*).*

7.3 Μη ντετερμινιστικά αυτόματα

Εισάγουμε τώρα μια παραλλαγή των ντετερμινιστικών αυτομάτων, τα *μη ντετερμινιστικά αυτόματα* (Non-deterministic Finite Automata ή NFA). Αυτά αποτελούν, φαινομενικά, μια ενίσχυση του μοντέλου των ντετερμινιστικών αυτομάτων, αφού, από τον ορισμό που θα δώσουμε, κάθε DFA θα είναι και NFA, και άρα οι γλώσσες που αναγνωρίζονται από τα NFA είναι ένα υπερσύνολο των γλωσσών που αναγνωρίζονται από DFA.

Θα δούμε όμως σύντομα ότι αυτό είναι μόνο φαινομενικό, και ότι τα δύο μοντέλα είναι απολύτως ισοδύναμα, όσον αφορά τουλάχιστον το ποιες γλώσσες αναγνωρίζουν. Με άλλα λόγια, θα δούμε μια μέθοδο που για κάθε NFA θα κατασκευάζει ένα ισοδύναμο DFA, ένα DFA δηλ. που θα αναγνωρίζει ακριβώς την ίδια γλώσσα με το δοθέν NFA. Παρ' όλα αυτα το να μελετούμε NFA προσφέρει μερικά πλεονεκτήματα σε σχέση με τα DFA σε ορισμένες περιπτώσεις, όπως θα δούμε στα παραδείγματα.

Ορισμός 7.8
(Μη ντετερμινιστικό Αυτόματο (NFA)) *Ένα* μη ντετερμινιστικό αυτόματο *είναι μια πεντάδα*

$$(Q, \Sigma, \delta, q_0, F)$$

όπου

- Q *είναι ένα πεπερασμένο σύνολο* καταστάσεων*,*
- Σ *είναι ένα πεπερασμένο αλφάβητο,*
- δ *είναι η* συνάρτηση μετάβασης *(transition function) με πεδίο ορισμού το* $Q \times \Sigma$ *και πεδίο τιμών το δυναμοσύνολο* 2^Q*, το σύνολο δηλ. όλων των υποσυνόλων του* Q*.*
- $q_0 \in Q$ *είναι μια από τις καταστάσεις που ονομάζεται* αρχική*, και*
- $F \subseteq Q$ *είναι το σύνολο των* τελικών *καταστάσεων.*

Ένα μη ντετερμινιστικό αυτόματο είναι σαν ένα DFA αλλά για κάθε κορυφή και για κάθε γράμμα του αλφαβήτου μπορεί κανεις να έχει οποιοδήποτε πεπερασμένο πλήθος από ακμές που ξεκινούν από την κορυφή και έχουν το γράμμα ως ετικέτα Μπορεί ακόμη και να μην υπάρχει καμία ακμή από κάποια κορυφή για κάποιο γράμμα. (Αν $\delta(q, \alpha) = \emptyset$ είναι το κενό σύνολο τότε δεν υπάρχει στο γράφημα καμία ακμή από την κορυφή q με ετικέτα α.)

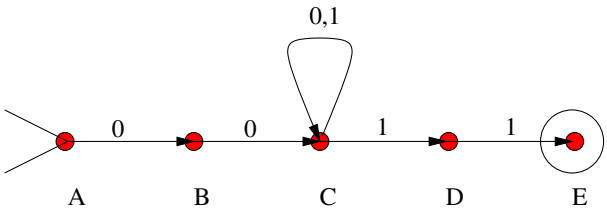
Η σημαντική διαφορά με πριν είναι ότι, όταν διαβάζουμε μια λέξη, δεν είναι πλέον μονοσήμαντα καθορισμένη η κίνησή μας πάνω στο γράφημα αφού ενδέχεται να έχουμε περισσότερες από μία επιλογές μετάβασης όντας σε μία κορυφή και διαβάζοντας ένα γράμμα. Το σε ποιες καταστάσεις μπορούμε να πάμε από μια κατάσταση $q \in Q$ αφού διαβάσουμε το γράμμα α μας το λέει η συνάρτηση μετάβασης. Το σύνολο αυτών των δυνατών καταστάσεων είναι το $\delta(q, \alpha) \subseteq Q$.

Παρατήρηση 7.4
Αν για μια κατάσταση q ενός NFA και για ένα γράμμα $\alpha \in \Sigma$ έχουμε $\delta(q, \alpha) = \emptyset$ αυτό ερμηνεύεται ως να μην είναι δυνατή η μετάβαση από την κατάσταση q προς οποιαδήποτε άλλη κατάσταση με το γράμμα α.

Ορισμός 7.9
(Αναγνώριση λέξης από NFA) *Θεωρούμε ότι μια λέξη $w = w_1 w_2 \dots w_n$, $w_j \in \Sigma$, αναγνωρίζεται από ένα NFA αν υπάρχει τρόπος να κινηθούμε, διαβάζοντας το w, πάνω στο γράφημα ώστε να καταλήξουμε σε τελική κορυφή. Ξεκινούμε ευρισκόμενοι στην αρχική κατάσταση q_0 και διαβάζουμε τα γράμματα w_1 έως w_n με αυτή τη σειρά. Κάθε φορά που διαβάζουμε ένα γράμμα w_j, και ευρισκόμενοι στην κατάσταση q, επιλέγουμε ως επόμενη κατάσταση μια από τις καταστάσεις του συνόλου $\delta(q, w_j)$. (Αν το σύνολο αυτό είναι κενό η λέξη απορρίπτεται.) Είναι φανερό ότι για κάθε λέξη υπάρχουν ενδεχομένως περισσότεροι από ένας τρόποι να κινηθούμε πάνω στο αυτόματο διαβάζοντας τα γράμματα αυτής της λέξης, αφού σε κάθε βήμα ενδέχεται να έχουμε τη δυνατότητα να επιλέξουμε την επόμενή μας κατάσταση. Απορρίπτεται η λέξη w αν και μόνο αν κανείς από τους δυνατούς τρόπους κίνησης δεν καταλήγει σε τελική κορυφή.*

Ορισμός 7.10
(Γλώσσα ενός NFA) *Το σύνολο των λέξεων που αποδέχεται το μη ντετερμινιστκό αυτόματο M ονομάζεται* η γλώσσα που αναγνωρίζει το αυτόματο *και συμβολίζεται με $L(M)$.*

Παράδειγμα 7.19
Το ακόλουθο παράδειγμα μη ντετερμινιστικού αυτομάτου αναγνωρίζει τη γλώσσα $00\{0,1\}^*11$.



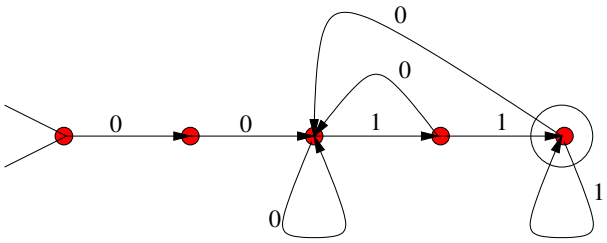
Σχήμα 7.6: NFA για τη γλώσσα $00\{0,1\}^*11$

Πρόκειται για NFA και όχι για DFA μια και στη μεσαία κορυφή υπάρχουν δύο ακμές με ετικέτα 1. Παρατηρήστε τη συντομογραφία που επιλέξαμε εδώ: ο βρόχος (loop) από τη μεσαία κορυφή στον εαυτό της έχει δύο ετικέτες 0 και 1. Αυτό σημαίνει ότι επιτρέπεται να διανύσουμε την κορυφή αυτή όταν διαβάσουμε είτε 0 είτε 1. Θα μπορούσαμε να είχαμε το ίδιο αποτέλεσμα αν φτιάχναμε δύο βρόχους από την κορυφή αυτή στον εαυτό της, ένα με ετικέτα 0 κι ένα με ετικέτα 1. Επιλέγουμε τη συντομογραφία για καθαρότητα στο σχήμα και τίποτε άλλο.

Γιατί το NFA του σχήματος 7.6 αναγνωρίζει τη γλώσσα $L = 00\{0,1\}^*11$; Παρατηρήστε ότι η L αποτελείται από εκείνες ακριβώς τις λέξεις που αρχίζουν με 00 και τελειώνουν με 11. Κάθε τέτοια λέξη περνάει από το NFA ως εξής: με τα δύο πρώτα 0 μεταβαίνει στη μεσαία κορυφή, στην οποία και παραμένει χρησιμοποιώντας το βρόχο μέχρι να διαβάσει και το προπροτελευταίο γράμμα. Με τα δύο τελευταία 1 επιλέγει να κινηθεί προς τα δεξιά για να καταλήξει στη μοναδική τελική κορυφή. Θα μπορούσε να επιλέξει με τα δύο τελευταία 1 να κινηθεί πάνω στο βρόχο της μεσαίας κορυφής, αλλά με αυτό τον τρόπο δεν καταλήγει σε τελική κορυφή. Αρκεί όμως για την αποδοχή μιας λέξης να υπάρχει έστω και ένας τρόπος να γίνει αποδεκτή.

Αντίστροφα τώρα, αν η λέξη w περνά από το NFA τότε υποχρεωτικά αρχίζει από δύο 0 (αλλιώς δε μπορεί να πάει δεξιότερα από τη δεύτερη κορυφή) και τελειώνει σε δύο 1 (αλλιώς δε μπορεί να καταλήξει στην τελική κορυφή).

Ας δώσουμε τώρα και ένα DFA για την ίδια γλώσσα:



Σχήμα 7.7: DFA για τη γλώσσα $00\{0,1\}^*11$

Είναι μια καλή άσκηση να να αποδείξετε ότι το άνω αυτόματο αναγνωρίζει τη γλώσσα $00\{0,1\}^*11$. Για να το κάνετε δώστε κάποιο «νόημα» στις καταστάσεις, όπως κάναμε παραπάνω για να δείξουμε ότι το DFA του σχήματος 7.5 δουλεύει.

Παρατήρηση 7.5
Συγκρίνοντας το NFA και το DFA για τη γλώσσα $00\{0,1\}^*11$ φαίνεται καθαρά το πλεονέκτημα του να σχεδιάζουμε NFA αντί για DFA. Επιτρέποντας στον εαυτό μας ένα πιο διευρυμένο μοντέλο μπορούμε να σχεδιάζουμε ευκολότερα αυτόματα για συγκεκριμένες γλώσσες, και η απλούστερη κατασκευή συνήθως επιτρέπει και μια ευκολότερη ανάλυση τού γιατί το συγκεκριμένο αυτόματο δουλεύει. Και, θα δούμε αργότερα, δε χάνεται τίποτα σχεδιάζοντας NFA αντί για DFA, γιατί αυτά τα δύο υπολογιστικά μοντέλα είναι ισοδύναμα. Όχι μόνο αυτό, αλλά ο τρόπος μετατροπής ενός NFA σε DFA μπορεί να είναι τελείως μηχανικός (αλγοριθμικός).

Παράδειγμα 7.20
Στο αυτόματο που φαίνεται στο σχήμα 7.6 παραπάνω έχουμε $Q = \{A, B, C, D, E\}$, $\Sigma = \{0, 1\}$, $q_0 = A$,

$F = \{E\}$, και

$$\begin{aligned}
\delta(A,0) &= \{B\} \\
\delta(A,1) &= \emptyset \\
\delta(B,0) &= \{C\} \\
\delta(B,1) &= \emptyset \\
\delta(C,0) &= \{C\} \\
\delta(C,1) &= \{C,D\} \\
\delta(D,0) &= \emptyset \\
\delta(D,1) &= \{E\} \\
\delta(E,0) &= \emptyset \\
\delta(E,1) &= \emptyset
\end{aligned}$$

✏ **7.16**
Κατασκευάστε ένα NFA που να αναγνωρίζει τη γλώσσα της άσκησης 7.11.

✏ **7.17**
Κατασκευάστε ένα NFA που να αναγνωρίζει εκείνες τις λέξεις πάνω από το $\Sigma = \{0,1\}$ που περιέχουν δύο μηδενικά που απέχουν μεταξύ τους στη λέξη κατά πολλαπλάσιο του 4. Δύο διαδοχικά μηδενικά θεωρούνται ότι απέχουν απόσταση μηδέν, άρα πολλαπλάσιο του 4.

7.4 Ισοδυναμία NFA και DFA.

Επαναλαμβάνουμε ότι για ένα NFA η συνάρτηση μετάβασης δ είναι ο τρόπος κωδικοποίησης των μεταβάσεων του. Αν δηλ. $q \in Q$ είναι μια κατάσταση και $\alpha \in \Sigma$ είναι ένα γράμμα του αλφαβήτου, το σύνολο $\delta(q,\alpha) \subseteq Q$ είναι το σύνολο όλων των καταστάσεων του NFA στις οποίες μπορεί αυτό να μεταβεί όντας στην κατάσταση q και διαβάζοντας το γράμμα α.

Ορισμός 7.11
(Η συνάρτηση δ πάνω σε σύνολα) *Αν $A \subseteq Q$ είναι ένα σύνολο καταστάσεων και $B \subseteq \Sigma$ είναι ένα σύνολο γραμμάτων τότε*

$$\delta(A,B) = \bigcup_{q\in A, \alpha\in B} \delta(q,\alpha).$$

Δηλ. $\delta(A,B)$ είναι το σύνολο όλων των καταστάσεων στις οποίες μπορεί κανείς να φτάσει ξεκινώντας από κάποια κατάσταση του A και ακολουθώντας κάποιο γράμμα α του συνόλου B. Η επέκταση αυτή της συνάρτησης δ ώστε να παίρνει ως όρισμα σύνολα αντί για γράμματα είναι η συνηθισμένη επέκταση μιας συνάρτησης $f : C \to D$ που με $f(X)$, $X \subseteq C$, συμβολίζει το σύνολο εικόνων του συνόλου X μέσω της f.

Επεκτείνουμε τώρα το πεδίο ορισμού της συνάρτησης δ όσον αφορά το δεύτερο όρισμά της.

Ορισμός 7.12
(Η συνάρτηση μετάβασης δ πάνω σε λέξεις) *Αν $q \in Q$ είναι μια κατάσταση και $w \in \Sigma^*$ είναι μια λέξη (ενδεχομένως και κενή) τότε ορίζουμε το σύνολο καταστάσεων $\delta(q, w)$ ως εξής:*

$$\delta(q,w) = \begin{cases} \{q\} & \epsilon\alpha\nu\ w = \epsilon \\ \delta(\delta(q,v),\alpha) & \epsilon\alpha\nu\ w = v\alpha, v \in \Sigma^*, \alpha \in \Sigma. \end{cases} \tag{7.1}$$

Παρατήρηση 7.6
Ο ορισμός (7.1) απαιτεί λίγη προσοχή όσον αφορά το δεύτερο σκέλος του μια και είναι αυτοαναφορικός*, αναφερόμαστε δηλ. στη συνάρτηση δ για να ορίσουμε τη συνάρτηση δ. Η ουσία εδώ είναι ότι αυτή η αυτοαναφορά δε δημιουργεί κάποιο πρόβλημα, μια και για να ορίσουμε το $\delta(q, w)$ αναφερόμαστε σε τιμές του $\delta(q, x)$ για λέξεις x με μήκος $|x| < |w|$, και υπάρχει και ο ξεχωριστός ορισμός για τη λέξη μήκους 0 όπου σταματά η αυτοαναφορά. Για να υπολογιστεί έτσι το $\delta(q, w)$ υπολογίζεται πρώτα το δ για ολοένα και μικρότερες λέξεις, ώσπου τελικά φτάνει να χρησιμοποιείται το πρώτο μέλος του ορισμού (7.1) που δεν έχει αυτοαναφορά. Για παράδειγμα, αν θέλει κανείς να υπολογίσει την τιμή $\delta(q, abc)$, όπου $a, b, c \in \Sigma$, ακολουθώντας τον ορισμό (7.1) αυτό γίνεται ως εξής:*

$$\begin{aligned} \delta(q,abc) &= \delta(\delta(q,ab),c) \\ &= \delta(\delta(\delta(q,a),b),c). \end{aligned}$$

Παρατηρούμε ότι στην τελευταία γραμμή η συνάρτηση δ είναι η γνωστή μας συνάρτηση που σαν δεύτερο όρισμα έχει σύμβολο του αλφαβήτου και όχι λέξη. Ορισμοί όπως ο (7.1) είναι πολύ κοινοί και ονομάζονται αναδρομικοί*.*

Με άλλα λόγια $\delta(q, w), w \in \Sigma^*$, είναι το σύνολο όλων εκείνων των καταστάσεων του αυτομάτου στις οποίες μπορεί κανείς να βρεθεί ξεκινώντας από την κατάσταση q και ακολουθώντας τη λέξη w. Και, αν $R \subseteq Q$ είναι ένα σύνολο καταστάσεων, με $\delta(R, w)$ συμβολίζεται το σύνολο όλων των καταστάσεων στις οποίες μπορεί κανείς να πάει ξεκινώντας από κάποια κατάσταση στο R και ακολουθώντας τη λέξη w.

Παρατήρηση 7.7
Μια λέξη w αναγνωρίζεται από ένα αυτόματο αν και μόνο αν

$$\delta(q_0, w) \cap F \neq \emptyset,$$

όπου F το σύνολο των τελικών καταστάσεων του NFA. Αναγνωρίζεται δηλ. μια λέξη αν και μόνο αν είναι δυνατή η μετάβαση *από την αρχική σε* κάποια *τελική κατάσταση ακολουθώντας τη λέξη.*

Ορισμός 7.13
(Ισοδυναμία αυτομάτων) *Δύο ντετερμινιστικά ή μη ντετερμινιστικά αυτόματα M_1 και M_2 λέγονται* ισοδύναμα *αν και μόνο αν $L(M_1) = L(M_2)$, αν αναγνωρίζουν δηλ. ακριβώς τις ίδιες λέξεις.*

Θεώρημα 7.1
(Ισοδυναμία NFA και DFA) *Για κάθε NFA M υπάρχει ισοδύναμο DFA M'.*

Απόδειξη

Περιγράφουμε ένα αλγόριθμο μετάβασης από ένα τυχόν NFA M σε ένα *ισοδύναμο* DFA M'.

Έστω λοιπόν ότι το NFA M είναι η πεντάδα $(Q, \Sigma, \delta, q_0, F)$. Το DFA $M' = (Q', \Sigma, \delta', q_0', F')$ θα έχει σύνολο καταστάσεων $Q' = 2^Q$ το δυναμοσύνολο (σύνολο όλων των υποσυνόλων) του Q, αρχική κατάσταση $q_0' = \{q_0\}$, ίδιο αλφάβητο Σ και τελικές καταστάσεις όλα εκείνα τα σύνολα καταστάσεων του M που περιέχουν κάποια τελική κατάσταση

$$F' = \{A \subseteq Q : A \cap F \neq \emptyset\}.$$

Τέλος η συνάρτηση μετάβασης $\delta' : Q' \times \Sigma \to Q'$ του M' ορίζεται ως

$$\delta'(q', \alpha) = \delta(q', \alpha).$$

Θυμηθείτε ότι το σύμβολο q' παριστάνει μια κατάσταση του M' άρα ένα σύνολο καταστάσεων του M, και άρα η δ συνάρτηση που εμφανίζεται δεξιά στον άνω ορισμό είναι η επεκτεταμένη δ συνάρτηση του αυτομάτου M όπως την ορίσαμε παραπάνω, μια και σαν πρώτο όρισμα έχει ολόκληρο σύνολο.

Με άλλα λόγια: στο DFA M' που κατασκευάζουμε από την κατάσταση q_1 (υποσύνολο του Q) με το σύμβολο $\alpha \in \Sigma$ μεταβαίνουμε στην κατάσταση q_2, που είναι το σύνολο όλων εκείνων των καταστάσεων του M στις οποίες μπορούμε να μεταβούμε από κάποια κατάσταση του συνόλου q_1 με το γράμμα α κινούμενοι πάνω στο M. Δείτε το Παράδειγμα 7.21 παρακάτω.

✏ **7.18**
Αποδείξτε με επαγωγή ως προς το μήκος $|w|$ της λέξης $w \in \Sigma^*$ ότι για κάθε κατάσταση q του M' ισχύει

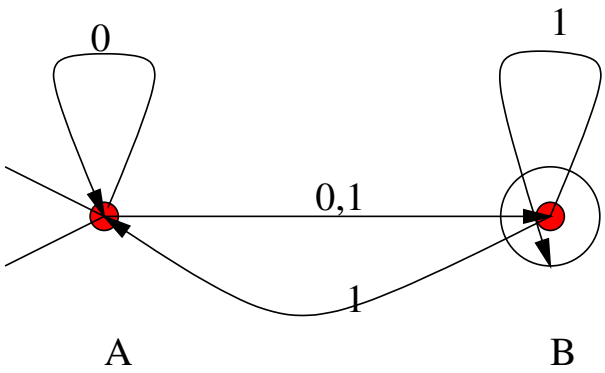
$$\delta'(q, w) = \delta(q, w).$$

Για να δείξουμε το Θεώρημα αρκεί να δείξουμε την ισοδυναμία

$$w \in L(M) \iff w \in L(M') \tag{7.2}$$

για όλες τις λέξεις $w \in \Sigma^*$. Αλλά $w \in L(M)$ αν και μόνο αν $\delta(q_0, w) \in F$, ενώ $w \in L(M')$ αν και μόνο αν $\delta'(q'_0, w) \in F'$. Χρησιμοποιώντας την Άσκηση 7.18 το τελευταίο συμβαίνει αν και μόνο αν $\delta(\{q_0\}, w) \in F'$ και, χρησιμοποιώντας τον ορισμό του F' βλέπουμε ότι αυτό ισχύει αν και μόνο αν $\delta(q_0, w) \cap F \neq \emptyset$. Όμως το σύνολο $\delta(q_0, w)$ είναι μονοσύνολο μια και το M είναι DFA, άρα η τελευταία συνθήκη είναι ισοδύναμη με $\delta(q_0, w) \in F$, και η απόδειξη είναι πλήρης.
■

Παράδειγμα 7.21
Ας δούμε τώρα πώς μετατρέπεται το ακόλουθο απλό NFA του Σχήματος 7.8 σε DFA. Το αποτέλεσμα δίνεται στο Σχήμα 7.9.

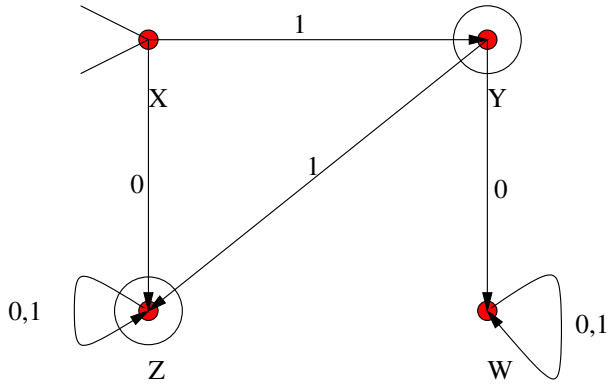


Σχήμα 7.8: M, ένα απλό NFA

Το σύνολο καταστάσεων του M' θα είναι το δυναμοσύνολο του συνόλου καταστάσεων του M δηλ. του $\{A, B\}$. Είναι δηλ. το σύνολο

$$Q' = \{X = \{A\}, Y = \{B\}, Z = \{A, B\}, W = \emptyset\}.$$

Σύνολο τελικών καταστασεων είναι το $F' = \{Y, Z\}$, όλα εκείνα τα σύνολα δηλ. που περιέχουν κάποια τελική κατάσταση του M. Αρχική κατάσταση είναι η X.



Σχήμα 7.9: Το NFA M του Σχήματος 7.8 μετετράπη στο DFA M'

✏ **7.19**
Ελέγξτε την ορθότητα την ισοδυναμίας του NFA του σχήματος 7.8 στο DFA του σχήματος 7.9, πάνω στις λέξεις 001 *και* 10.

✏ **7.20**
Φτιάξτε ισοδύναμα DFA για τα NFA

1. $(Q = \{p, q, r, s\}, \Sigma = \{0, 1\}, \delta_1, q_0 = p, F = \{s\})$
2. $(Q = \{p, q, r, s\}, \Sigma = \{0, 1\}, \delta_2, q_0 = p, F = \{q, s\})$

όπου οι συναρτήσεις μετάβασης είναι οι

δ_1 :

	0	1
p	$\{p, q\}$	$\{p\}$
q	$\{r\}$	$\{r\}$
r	$\{s\}$	$\emptyset$
s	$\{s\}$	$\{s\}$

δ_2 :

	0	1
p	$\{q, s\}$	$\{q\}$
q	$\{r\}$	$\{q, r\}$
r	$\{s\}$	$\{p\}$
s	$\emptyset$	$\{p\}$

✏ **7.21**
Αν ένα NFA έχει n σε πλήθος καταστάσεις, πόσες το πολύ καταστάσεις χρειάζεται να έχει ένα ισοδύναμό του DFA;

7.5 NFA με ε-κινήσεις

Μια ακόμη παραλλαγή του μοντέλου του πεπερασμένου αυτομάτου είναι το μη ντετερμινιστικό αυτόματο με ϵ-κινήσεις. Αυτό είναι ένα NFA που έχει, ενδεχομένως, και κάποιες ακμές που αντί να έχουν ως ετικέτα ένα γράμμα του αλφαβήτου έχουν την κενή λέξη ϵ. Κινούμενοι πάνω στο αυτόματο αυτό για να αναγνωρίσουμε μια λέξη έχουμε το δικαίωμα να διανύσουμε μια ϵ-ακμή οποτεδήποτε υπάρχει μια τέτοια από την τρέχουσα κατάσταση *χωρίς να μας ενδιαφέρει ποιο είναι το επόμενο γράμμα της λέξης*. Η διάνυση μιας ϵ-ακμής *δε συνοδεύεται από μεταπήδηση στο επόμενο γράμμα της λέξης*. Ας τα λέμε αυτά ϵ-NFA.

Ορισμός 7.14
(Μη ντετερμινιστικό αυτόματο με ϵ-κινήσεις (ϵ-NFA)) *Ένα* μη ντετερμινιστικό αυτόματο *με ϵ-κινήσεις (ϵ-NFA) είναι μια πεντάδα*

$$(Q, \Sigma, \delta, q_0, F)$$

όπου

- *Q είναι ένα πεπερασμένο σύνολο* καταστάσεων,
- *Σ είναι ένα πεπερασμένο αλφάβητο,*
- *δ είναι η* συνάρτηση μετάβασης *(transition function) με πεδίο ορισμού το $Q \times (\Sigma \cup \{\epsilon\})$ και πεδίο τιμών το δυναμοσύνολο 2^Q, το σύνολο δηλ. όλων των υποσυνόλων του Q.*
- *$q_0 \in Q$ είναι μια από τις καταστάσεις που ονομάζεται* αρχική, *και*
- *$F \subseteq Q$ είναι το σύνολο των* τελικών *καταστάσεων.*

Παρατήρηση 7.8
Η ουσιαστική διαφορά από τον ορισμό του NFA είναι ότι η συνάρτηση μετάβασης μπορεί να έχει και το ϵ ως δεύτερο όρισμα και όχι απαραίτητα ένα γράμμα του αλφαβήτου Σ.

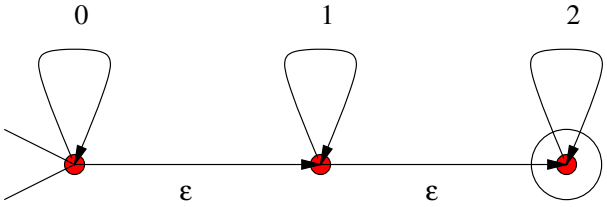
Παρατήρηση 7.9
Το νόημα μιας ϵ-ακμής από μια κορυφή q_1 σε μια κορυφή q_2 είναι το εξής: αν το NFA βρίσκεται στην κατάσταση q_1 τότε μπορεί να επιλέξει να μεταβεί στην κατάσταση q_2 χωρίς να διαβάσει το επόμενο γράμμα της λέξης.

Ορισμός 7.15
(Αναγνώριση λέξης από ϵ-NFA) *Θεωρούμε ότι μια λέξη $w = w_1 w_2 \dots w_n$, $w_j \in \Sigma$, αναγνωρίζεται από ένα ϵ-NFA αν υπάρχει τρόπος να κινηθούμε, διαβάζοντας το w, πάνω στο γράφημα ώστε να καταλήξουμε σε τελική κορυφή. Ξεκινούμε ευρισκόμενοι στην αρχική κατάσταση q_0 και διαβάζουμε τα γράμματα w_1 έως w_n με αυτή τη σειρά. Σε κάθε βήμα έχουμε τη δυνατότητα να διαβάσουμε το επόμενο γράμμα w_j και να εκτελέσουμε μια μετάβαση σε νέα κατάσταση ή όχι.*

Κάθε φορά που διαβάζουμε ένα γράμμα w_j, και ευρισκόμενοι στην κατάσταση q, επιλέγουμε ως επόμενη κατάσταση μια από τις καταστάσεις του συνόλου $\delta(q, w_j)$. (Αν το σύνολο αυτό είναι κενό η λέξη απορρίπτεται.) Αν επιλέξουμε να μη διαβάσουμε το επόμενο γράμμα της λέξης μπορούμε να μεταβούμε σε νέα κατάσταση ακολουθώντας μια ϵ-ακμή, μπορούμε δηλ. να μεταβούμε σε μια οποιαδήποτε από τις καταστάσεις του συνόλου $\delta(q, \epsilon)$, όπου q είναι η τρέχουσα κατάσταση. (Αν το σύνολο αυτό είναι κενό η λέξη απορρίπτεται.) Είναι φανερό ότι για κάθε λέξη υπάρχουν ενδεχομένως περισσότεροι από ένας τρόποι να κινηθούμε πάνω στο αυτόματο διαβάζοντας τα γράμματα αυτής της λέξης, αφού σε κάθε βήμα ενδέχεται να έχουμε τη δυνατότητα να επιλέξουμε την επόμενή μας κατάσταση. Απορρίπτεται η λέξη w αν και μόνο αν κανείς από τους δυνατούς τρόπους κίνησης δεν καταλήγει σε τελική κορυφή.

Ορισμός 7.16
(Γλώσσα ενός ϵ-NFA) *Το σύνολο των λέξεων που αποδέχεται το μη ντετερμινιστικό αυτόματο με ϵ κινήσεις M ονομάζεται* η γλώσσα που αναγνωρίζει το αυτόματο *και συμβολίζεται με $L(M)$.*

Παράδειγμα 7.22
Το ϵ-NFA του Σχήματος 7.10 αναγνωρίζει τη γλώσσα $0^*1^*2^*$.



Σχήμα 7.10: Ένα ϵ-NFA για τη γλώσσα $0^*1^*2^*$.

Για παράδειγμα, πώς αναγνωρίζει τη λέξη $0^2 1^3 2^5$ (συντομογραφία για τη λέξη 0011122222); Κάνει δύο μεταβάσεις από την πρώτη κορυφή στον εαυτό της διαβάζοντας τα δύο 0, μετά μεταβαίνει στη δεύτερη

κορυφή χωρίς να διαβάσει τίποτα, *μεταβαίνει από τη δεύτερη κορυφή στον εαυτό της τρεις φορές διαβάζοντας τα 1, μεταβαίνει στην τρίτη κορυφή χωρίς πάλι να διαβάσει τίποτα, και τέλος μεταβαίνει από την τρίτη κορυφή στον εαυτό της διαβάζοντας τα πέντε 2.*

✏ **7.22**
Κατασκευάστε ένα ϵ-NFA που να αναγνωρίζει τη γλώσσα $(0101)^* \cup (111)^*$.

✏ **7.23**
Αν M_1 και M_2 είναι δύο DFA περιγράψτε πως θα τα χρησιμοποιήσετε αυτά για να κατασκευάσετε ένα ϵ-NFA για τη γλώσσα $L(M_1) \cup L(M_2)$.
Χρησιμοποιήστε τα M_1 και M_2 βάζοντας πριν από αυτά μια κοινή κατάσταση εισόδου με ϵ-κινήσεις μόνο προς τα δύο DFA.

✏ **7.24**
Αν M_1 και M_2 είναι δύο DFA περιγράψτε πως θα τα χρησιμοποιήσετε αυτά για να κατασκευάσετε ένα ϵ-NFA για τη γλώσσα $L(M_1)L(M_2)$. Αν το M_1 έχει ακριβώς μια τελική κατάσταση κατασκευάστε DFA για τη γλώσσα αυτή.
Χρησιμοποιήστε το M_1 ακολουθούμενο από το M_2. Από τις τελικές καταστάσεις του M_1 θα φεύγουν κάποιες ϵ-ακμές.

7.6 Ισοδυναμία ε-NFA και NFA

Εδώ θα αποδείξουμε ότι τα ϵ-NFA είναι ισοδύναμα με τα NFA, και άρα και με τα DFA. Για κάθε ϵ-NFA δηλ. υπάρχει ένα NFA χωρίς ϵ-κινήσεις που αναγνωρίζει την ίδια γλώσσα.

Ορισμός 7.17
(ϵ-μονοπάτι) *Ένα* ϵ-μονοπάτι *στο γράφημα ενός ϵ-NFA είναι μια πεπερασμένη ακολουθία διαδοχικών ϵ-ακμών (ακμών δηλ. που φέρουν την ετικέτα ϵ).*

Ορισμός 7.18
(α-μονοπάτι) *Ένα* α-μονοπάτι, *όπου $\alpha \in \Sigma$, είναι ένα μονοπάτι στο γράφημα ενός ϵ-NFA που απαρτίζεται από ένα αρχικό ϵ-μονοπάτι, ακολουθούμενο από μια ακμή με ετικέτα α, ακολουθούμενο από ένα ϵ-μονοπάτι. Τα δύο ϵ-μονοπάτια μπορούν να είναι και κενά.*

Θεώρημα 7.2
(Ισοδυναμία ϵ-NFA και NFA) *Για κάθε ϵ-NFA M υπάρχει ισοδύναμο NFA M'.*

Απόδειξη

Για να μεταβούμε από ένα ϵ-NFA M σε ένα ισοδύναμο NFA M' κάνουμε τα εξής:

- Το σύνολο καταστάσεων του M' είναι ίδιο με του M.
- Η αρχική κατάσταση του M' είναι ίδια με αυτή του M.
- Οι τελικές καταστάσεις του M', το σύνολο των οποίων συμβολίζουμε με F', είναι όλες εκείνες τις καταστάσεις από τις οποίες μπορούμε να φτάσουμε σε κάποια κορυφή του F (το σύνολο τελικών καταστάσεων του M) με ένα ϵ-μονοπάτι. Επειδή ένα κενό μονοπάτι είναι ϵ-μονοπάτι, ο ορισμός αυτός συνεπάγεται ότι $F \subseteq F'$.
- Για κάθε κατάσταση q και γράμμα $\alpha \in \Sigma$ θέτουμε στο M' ως $\delta_{M'}(q, \alpha)$ το σύνολο όλων των καταστάσεων στις οποίες μπορεί κανείς να μεταβεί από την q στο M διανύοντας κάποιο α-μονοπάτι.
- Καταργούμε όλες τις ϵ-κινήσεις.

Έστω τώρα $w = w_1 w_2 \cdots w_n \in \Sigma^*$, $n \geq 0$. Πρέπει να δείξουμε ότι η λέξη w γίνεται δεκτή από το M αν και μόνο αν γίνεται δεκτή από το M.

Αν $w \in L(M)$ αυτό σημαίνει ότι υπάρχει τρόπος κίνησης πάνω στο M, διαβάζοντας τα γράμματα της λέξης w είτε ακολουθώντας ϵ-κινήσεις, ώστε να μεταβούμε από την q_0 σε κάποια κατάσταση $f \in F$. Σε αυτή την περίπτωση δείχνουμε ότι υπάρχει τρόπος κίνησης πάνω στο M τέτοιος που να οδηγεί από την q_0 σε κάποια κατάσταση του F'.

Έστω λοιπόν ότι $w \in L(M)$. Αυτό σημαίνει ότι υπάρχει μια ακολουθία καταστάσεων του M έστω $q_0, q_1, \ldots, q_{k-1}, q_k$, $k \geq 0$, τέτοια ώστε $q_k \in F$ και η μετάβαση από την q_j στην q_{j+1}, $0 \leq j < k$, γίνεται είτε με κάποιο γράμμα w_j είτε με μια ϵ-ακμή, και τα γράμματα w_j χρησιμοποιούνται όλα, από μια φορά το καθένα, και με τη σειρά.

Χωρίζουμε την πεπερασμένη αυτή ακολουθία των μεταβάσεων $q_0 \to q_1, q_1 \to q_2, \ldots, q_{k-1} \to q_k$ σε κομμάτια $q_{a_0} \to q_{a_1}, q_{a_1} \to q_{a_2}, \ldots, q_{a_{n-1}} \to q_{a_n}$ (με $a_0 = 0$, $a_n = k$) τα οποία αντιστοιχούν σε ένα w_1-μονοπάτι, ακολουθούμενο από ένα w_2-μονοπάτι, κλπ., τελειώνοντας με ένα w_n-μονοπάτι. Από τον ορισμό του NFA M' προκύπτει ότι στο M' είναι δυνατή η μετάβαση από την κορυφή q_{a_0} στην q_{a_1} με μια w_1-ακμή, από την q_{a_1} στην q_{a_2} με μια w_2-ακμή, κλπ. Επειδή η κατάσταση q_k παραμένει τελική κατάσταση και του M' προκύπτει ότι $w \in L(M')$.

Ο εγκλεισμός $L(M') \subseteq L(M)$ αφήνεται ως άσκηση (Άσκηση 7.25).

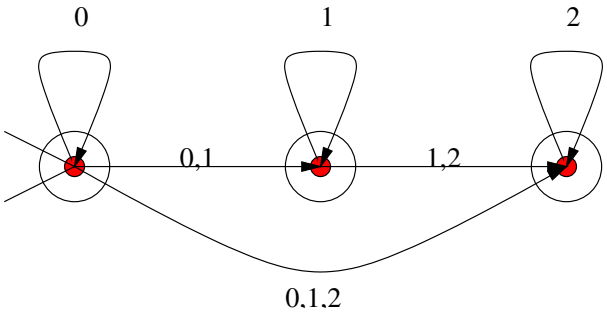
■

✏ **7.25**

Με το συμβολισμό της άνω απόδειξης δείξτε ότι αν μια λέξη αναγνωρίζεται από το NFA M' τότε αναγνωρίζεται και από το ϵ-NFA M.

Παράδειγμα 7.23

Με τη μέθοδο της απόδειξης του Θεωρήματος 7.2 το ϵ-NFA του Σχήματος 7.10



Σχήμα 7.11: Το ϵ-NFA του Σχήματος 7.10 όπως έχει μετατραπεί σε NFA

μετατρέπεται στο NFA του Σχήματος 7.11.

7.7 Κανονικές εκφράσεις και οι γλώσσες τους

Οι κανονικές εκφράσεις που θα δούμε σε αυτή την παράγραφο είναι ένας διαφορετικός τρόπος περιγραφής μιας γλώσσας που αναγνωρίζεται από ένα DFA. Είναι μάλιστα ένας αρκετά πιο συνοπτικός και διαισθητικός τρόπος να περιγράψει κανείς μια τέτοια γλώσσα και γι' αυτό το λόγο είναι ένας τρόπος που χρησιμοποιείται πολύ στην πράξη.

Θα δώσουμε κατ' αρχήν ένα αναδρομικό ορισμό για το τι είναι μια *κανονική έκφραση* (regular expression) και το ποια γλώσσα παριστάνει.

Ορισμός 7.19

(Κανονικές εκφράσεις και οι γλώσσες τους) *Οι παρακάτω λέξεις ορίζονται να είναι* κανονικές εκφράσεις *με τις αντίστοιχες γλώσσες. (Με $L(\cdot)$ συμβολίζουμε τη* γλώσσα μιας έκφρασης.*)*

- $\emptyset$, *και* $L(\emptyset) = \emptyset$ *(η κενή γλώσσα, που δεν περιέχει καμία λέξη)*
- ϵ, *και* $L(\epsilon) = \{\epsilon\}$ *(η γλώσσα που περιέχει μόνο μια λέξη, την κενή λέξη* ϵ*)*
- α, *για κάθε* $\alpha \in \Sigma$, *και* $L(\alpha) = \{\alpha\}$.

Επίσης, αν r *και* s *είναι κανονικές εκφράσεις τότε και οι ακόλουθες λέξεις είναι επίσης κανονικές εκφράσεις.*

1. (r), *και* $L((r)) = L(r)$.
2. $(r + s)$, *και* $L((r + s)) = L(r) \cup L(s)$,
3. (rs), *και* $L((rs)) = L(r)L(s)$,
4. (r^*), *και* $L((r^*)) = L(r)^*$.

Μια γλώσσα L *λέγεται κανονική αν υπάρχει κανονική έκφραση* r *με* $L = L(r)$.

Παρατήρηση 7.10
Αν μπορούμε να παρελείψουμε τις παρανθέσεις χωρίς να αλλάξουμε το νόημα τότε το κάνουμε αυτό. Λαμβάνουμε υπόψιν ότι τη μεγαλύτερη προτεραιότητα έχει ο εκθέτης $*$*, μετά έρχεται η συγκόλληση και τέλος η πρόσθεση. Για παράδειγμα η κανονική έκφραση* $01^* + 10^*$ *ερμηνεύεται ως* $(0(1^*)) + (1(0^*))$. *Αν* r *είναι μια κανονική έκφραση τότε χρησιμοποιούμε επίσης τη συντομογραφία* r^+ *αντί για* rr^*.

Παράδειγμα 7.24
Τα παρακάτω είναι παραδείγματα κανονικών εκφράσεων και των γλωσσών τους.

Κανονική έκφραση	**Αντίστοιχη γλώσσα**
00	$\{00\}$
$(0 + 1)^*$	*Όλες οι λέξεις πάνω από το* $\Sigma = \{0, 1\}$
$(0 + 1)^*00(0 + 1)^*$	*Όλες οι λέξεις πάνω από το* $\Sigma = \{0, 1\}$ *που έχουν δύο διαδοχικά μηδενικά*
$(1 + 10)^*$	*Ότι αρχίζει με 1 και δεν έχει διαδοχικά 0*
$(0 + \epsilon)(1 + 10)^*$	*Ότι δεν έχει διαδοχικά 0*
$0^*1^*2^*$	*Λέξεις όπου τα 0 έρχονται πριν τα 1 κι αυτά πριν τα 2.*

✏ **7.26**
Γράψτε κανονικές εκφράσεις για τις ακόλουθες γλώσσες:

1. *Λέξεις που δεν περιέχουν τη μορφή 101.*
2. *Λέξεις όπου όλες οι εμφανίσεις διαδοχικών 0 συμβαίνουν πριν από οποιαδήποτε εμφάνιση διαδοχικών 1.*

✏ **7.27**
Περιγράψτε τις γλώσσες που ορίζονται από τις κανονικές εκφράσεις:

1. $(11 + 0)^*(00 + 1)^*$
2. $(1 + 01 + 001)^*(\epsilon + 0 + 00)^*$
3. $(00 + 11 + (01 + 10)(00 + 11)^*(01 + 10))^*$

✏ **7.28**
Δείξτε τις παρακάτω ταυτότητες όπου r, s, t *είναι οποιεσδήποτε κανονικές εκφράσεις. Η ισότητα παρακάτω δε σημαίνει ότι οι δύο εκφράσεις είναι ίσες (και δεν είναι, μια και οι εκφράσεις είναι λέξεις, και ως τέτοιες διαφέρουν) αλλά ότι οι αντίστοιχες γλώσσες είναι ίσες.*

1. $r + s = s + r$

2. $(r+s)+t = r+(s+t)$
3. $(rs)t = r(st)$
4. $r(s+t) = rs+rt$
5. $(r+s)t = rt+st$
6. $\emptyset^* = \epsilon$
7. $(r^*)^* = r^*$
8. $(\epsilon + r)^* = r^*$
9. $(r^*s^*)^* = (r+s)^*$

7.8 Κανονικότητα γλωσσών των αυτομάτων

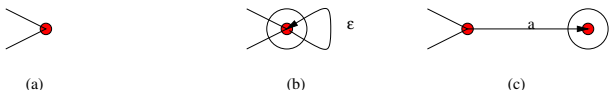
Η βασική πρόταση είναι η ακόλουθη.

Θεώρημα 7.3
(Κανονικότητα γλωσσών των αυτομάτων) *Μια γλώσσα είναι κανονική αν και μόνο αν αναγνωρίζεται από κάποιο αυτόματο.*

Παρατήρηση 7.11
Παρατηρήστε ότι στο Θεώρημα 7.3 δεν ξεκαθαρίζουμε για τι είδους αυτόματο μιλάμε. Έχουμε όμως ήδη αποδείξει ότι κάθε ϵ-NFA είναι ισοδύναμο με κάποιο NFA και κάθε NFA με κάποιο DFA. Αυτό σημαίνει ότι μια γλώσσα αναγνωρίζεται από ένα αυτόματο κάποιου είδους από τα τρία αν και μόνο αν αναγνωρίζεται από αυτόματο οποιουδήποτε είδους.

Απόδειξη

Θα δείξουμε ότι (α) Κάθε κανονική γλώσσα αναγνωρίζεται από κάποιο ϵ-NFA, και (β) Η γλώσσα που αναγνωρίζει κάθε DFA είναι κανονική.
(α) Χρησιμοποιούμε επαγωγή ως προς το μήκος της κανονικής έκφρασης r που παράγει τη γλώσσα. Αν πρόκειται για μια από τις εκφράσεις $\emptyset$, ϵ ή a, με $a \in \Sigma$, πολύ εύκολα φτιάχνουμε αυτόματα που τις αναγνωρίζουν όπως φαίνεται στο παρακάτω Σχήμα 7.12.

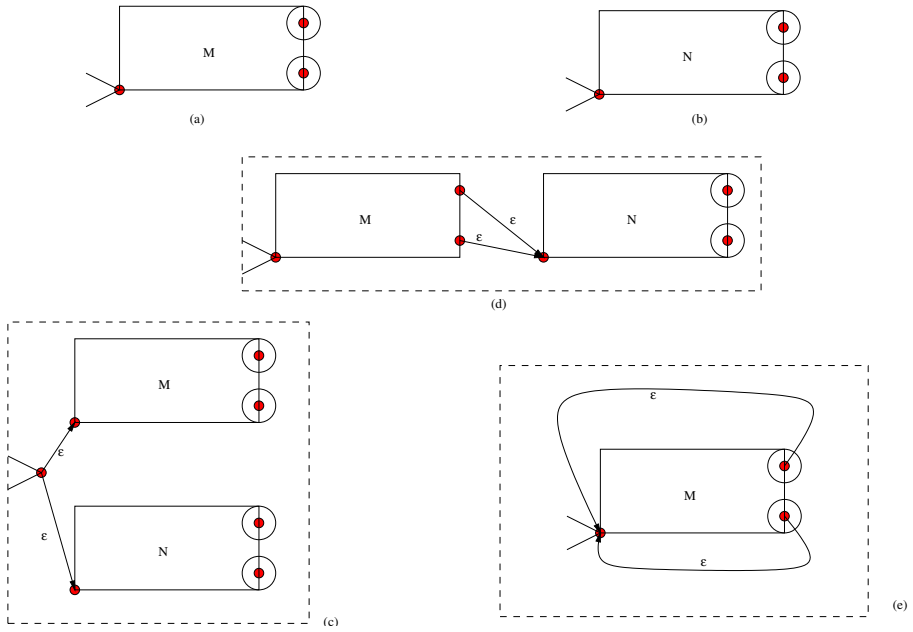


Σχήμα 7.12: Τα ϵ-NFA για τις εκφράσεις $\emptyset$ (a), ϵ (b) και a (c)

Αν τώρα έχουμε μια έφραση x του τύπου $r+s$, rs η r^*, τότε τα μήκη των r και s είναι αυστηρά μικρότερα του $|x|$, άρα μπορούμε να υποθέσουμε επαγωγικά ότι έχουμε κάποια αυτόματα M και N που αναγνωρίζουν τις γλώσσες $L(r)$ και $L(s)$. Χρησιμοποιούμε τα M και N σα μαύρα κουτιά και μας ενδιαφέρει μόνο να «βλέπουμε» απ' έξω τις αρχικές και τελικές τους καταστάσεις.

Στο Σχήμα 7.13 βλέπουμε στα (a) και (b) τα αυτόματα M και N που αντιστοιχούν στις εκφράσεις r και s. Στα (c), (d) και (e) βλέπουμε πως αυτά συνδυάζονται ώστε να φτιάξουν αυτόματα για τις γλώσσες $r+s$, rs και r^*.

Στο (c) ορίζουμε μια νέα αρχική κορυφή και την ενώνουμε με ϵ-ακμές με τις δύο αρχικές κορυφές των M και N. Οι τελικές καταστάσεις παραμένουν οι ίδιες.



Σχήμα 7.13: (a) Αυτόματο για r, (b) για s, (c) για $r+s$, (d) για rs, (e) για r^*

Στο (d) αρχική κορυφή είναι αυτή του M του οποίου οι τελικές καταστάσεις συνδέονται με ϵ-ακμές με την αρχική του N. Τελικές καταστάσεις του συμπλέγματος είναι αυτές του N.

Στο (e) οι τελικές καταστάσεις του M συνδέονται με ϵ-ακμές με την αρχική κατάσταση του M. Αρχικές και τελικές καταστάσεις παραμένουν οι ίδιες.

(β) Έστω DFA $M = (Q, \Sigma, \delta, q_1, F)$, όπου $Q = \{q_1, \ldots, q_n\}$. Ορίζουμε για $i, j = 1, \ldots, n$, $k = 0, \ldots, n$, τις γλώσσες $R^k_{i,j}$ να είναι εκείνες οι λέξεις του Σ^* που είναι τέτοιες ώστε αν ξεκινήσουμε από την κορυφή q_i και τις ακολουθήσουμε τότε φτάνουμε στην κορυφή q_j **χωρίς να χρησιμοποιήσουμε κορυφή** q_l **με** $l > k$**.**

Είναι φανερό ότι

$$L(M) = \bigcup_{q_j \in F} R^n_{1,j}. \tag{7.3}$$

Με άλλα λόγια, αποδεκτές γίνονται εκείνες οι λέξεις που μας επιτρέπουν να φτάσουμε, ξεκινώντας από την αρχική κορυφή q_1, σε κάποια από τις κορυφές $q_j \in F$, χωρίς κανένα περιορισμό ως προς τις ενδιάμεσες κορυφές (επειδή ο άνω δείκτης είναι n, και, ούτως ή άλλως, δεν υπάρχουν κορυφές q_l, με $l > n$.

Θα δείξουμε με επαγωγή ως προς το k ότι οι γλώσσες $R^k_{i,j}$ είναι όλες κανονικές. Άρα κανονική είναι και η $L(M)$ αφού με βάση την (7.3) είναι **πεπερασμένη** ένωση από κανονικές γλώσσες, και η ένωση δύο κανονικών γλωσσών είναι εξ ορισμού κανονική.

Για $k = 0$ τώρα, παρατηρούμε ότι η απαίτηση, στον ορισμό της $R^k_{i,j}$ όσον αφορά το ποιες κορυφές δεν πρέπει να χρησιμοποιηθούν είναι ιδιαίτερα αυστηρή, αφού η συνθήκη $l > 0$ ισχύει για κάθε κορυφή $q_l \in Q$. Άρα έχουμε

$$R^0_{i,j} = \begin{cases} \{\alpha \in \Sigma : \ \delta(q_i, \alpha) = q_j\} & (i \neq j) \\ \{\alpha \in \Sigma : \ \delta(q_i, \alpha) = q_i\} \cup \{\epsilon\} & (i = j) \end{cases}$$

Αυτό σημαίνει ότι οι γλώσσες $R^0_{i,j}$ είναι πεπερασμένα σύνολα από σύμβολα του Σ ή το γράμμα ϵ. Κάθε ένα όμως από αυτά είναι κανονική γλώσσα άρα είναι τέτοια και η $R^0_{i,j}$.

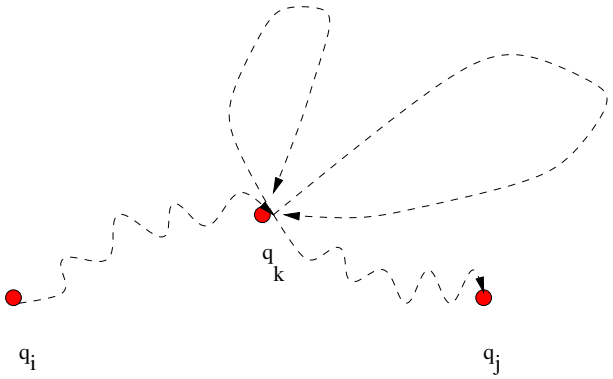
Όσον αφορά το επαγωγικό βήμα, αν υποθέσουμε ότι οι $R^{k-1}_{i,j}$ είναι όλες κανονικές τότε το ίδιο

συνάγουμε και για τις $R^k_{i,j}$ αφού παρατηρήσουμε ότι ισχύει η αναδρομική σχέση

$$R^k_{i,j} = R^{k-1}_{i,k}(R^{k-1}_{k,k})^* R^{k-1}_{k,j} \cup R^{k-1}_{i,j}. \tag{7.4}$$

Γιατί όμως ισχύει η (7.4);

Είναι φανερό ότι η γλώσσα $R^k_{i,j}$ είναι υπερσύνολο της $R^{k-1}_{i,j}$, αφού ο περιορισμός $l \leq k$, στον ορισμό της $R^k_{i,j}$, γίνεται ασθενέστερος (ισχύει πιο συχνά) όσο μεγαλώνει το k. Ποιες είναι όμως εκείνες οι λέξεις που ανήκουν στο σύνολο $R^k_{i,j}$ αλλά όχι στο $R^{k-1}_{i,j}$, οι λέξεις με άλλα λόγια της (συνολοθεωρητικής) διαφοράς $R^k_{i,j} \setminus R^{k-1}_{i,j}$; Είναι ακριβώς εκείνες οι λέξεις που οδηγούν από την κατάσταση q_i στην q_j, χωρίς να «πατούν» σε κορυφή q_l, $l > k$, αλλά που πατούν τουλάχιστον μια φορά στην κορυφή q_k όως φαίνεται στο Σχήμα 7.14.



Σχήμα 7.14: Ένα μονοπάτι στο DFA που αντιστοιχεί σε λέξη του $R^k_{i,j} \setminus R^{k-1}_{i,j}$

Μια τέτοια λέξη αντιστοιχεί σε ένα μονοπάτι πάνω στο DFA που σίγουρα «πατάει» πάνω στην κορυφή q_k, ενδεχομένως και πάνω από μία φορά (στο Σχήμα 7.14 πατάει δύο φορές). Αν ονομάσουμε w μια τέτοια λέξη, και ονομάσουμε σ το πρόθεμα της w που αντιστοιχεί στο μονοπάτι από το q_i στο q_k, που δεν πατάει στην q_k, και τ το επίθεμα της w γαι το μονοπάτι $q_k \to q_j$ που δεν πατάει στην q_k, τότε η w γράφεται

$$w = \sigma v_1 \cdots v_t \tau,$$

όπου οι λέξεις $v_1, \ldots, v_t$ αντιστοιχούν σε μονοπάτια που αρχίζουν και τελειώνουν από το q_k, χωρίς να πατούν στο q_k. Είναι δηλ. $\sigma \in R^{k-1}_{i,k}$, $v_l \in R^{k-1}_{k,k}$, $l = 1, \ldots, t$, και $\tau \in R^{k-1}_{k,j}$, έχουμε άρα δείξει τον εγκλεισμό

$$R^k_{i,j} \setminus R^{k-1}_{i,j} \subseteq R^{k-1}_{i,k}(R^{k-1}_{k,k})^* R^{k-1}_{k,j}.$$

Ο αντίστροφος εγκλεισμός είναι ακόμη πιο εύκολος και παραλείπεται.

■

✏ **7.29**

Κατασκευάστε DFA για τις κανονικές εκφράσεις:

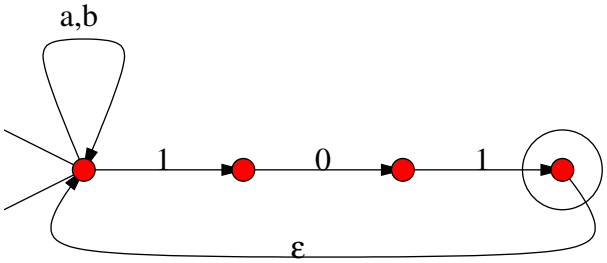
1. $10 + (0 + 11)0^*1$
2. $01\,(((10)^* + 111)^* + 0)^*\,1$
3. $((0 + 1)(0 + 1))^* + ((0 + 1)(0 + 1)(0 + 1))^*$

✏ **7.30**

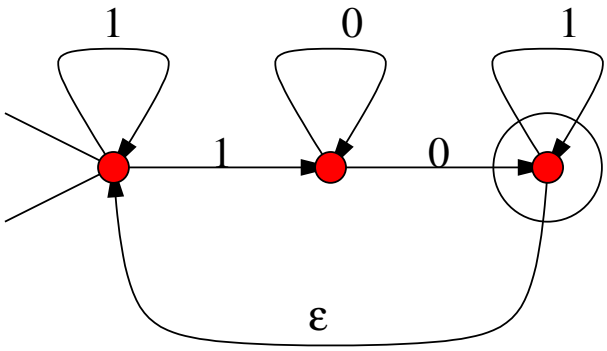
Δώστε μια κανονική έκφραση για τη γλώσσα που αναγνωρίζει το αυτόματο του Σχήματος 7.15.

✏ **7.31**

Δώστε μια κανονική έκφραση για τη γλώσσα που αναγνωρίζει το αυτόματο του Σχήματος 7.16.



Σχήμα 7.15: Το Σχήμα για την Άσκηση 7.30



Σχήμα 7.16: Το Σχήμα για την Άσκηση 7.31

7.9 Κλειστότητα κανονικών γλωσσών κάτω από απλές πράξεις

Από τον ορισμό των κανονικών εκφράσεων και των γλωσσών είναι φανερό ότι αν L_1 και L_2 είναι κανονικές γλώσσες τότε κανονική είναι και η $L_1 \cup L_2$ όπως και η γλώσσα L_1^*. Δεν είναι όμως καθόλου προφανές από τον ορισμό των κανονικών εκφράσεων το αν η συμπληρωματική γλώσσα

$$L_1^c = \{w \in \Sigma^* : \ w \notin L_1\}$$

είναι κανονική. Γίνεται όμως και αυτό φανερό αν χρησιμοποιήσουμε το Θεώρημα 7.3 που λέει ότι μια γλώσσα είναι κανονική αν και μόνο αν υπάρχει ένα DFA που την αναγνωρίζει. Έστω λοιπόν ότι το DFA M αναγνωρίζει τη γλώσσα L_1. Φτιάνχουμε ένα DFA M' από το M κρατώντας τις ίδιες καταστάσεις, αλφάβητο, αρχική κατάσταση και ακμές του M αλλά κάνουμε όλες τις τελικές καταστάσεις του M μη τελικές και όλες τις μη τελικές καταστάσεις του M τις κάνουμε τελικές στο M'. (Εδώ πρέπει να είμαστε λίγο προσεκτικοί και να δουλεύουμε στο μορφή του M που δε χρησιμοποιεί συντομογραφία, αλλά που ικανοποιεί την αρχική απαίτηση για DFA, ότι δηλ. για κάθε κατάσταση και για κάθε γράμμα του αλφαβήτου υπάρχει ακριβώς μια ακμή.) Είναι φανερό τώρα ότι μια λέξη γίνεται δεκτή στο M' αν και μόνο αν *δε γίνεται δεκτή στο* M, άρα το M' είναι ένα DFA για τη γλώσσα L_1^c.

Είναι τώρα εύκολο να δείξουμε ότι και η γλώσσα $L_1 \cap L_2$ είναι κανονική. Αρκεί να δείξουμε ότι το συμπλήρωμά της είναι, και

$$(L_1 \cap L_2)^c = L_1^c \cup L_2^c,$$

και από αυτά που είπαμε προηγουμένως προκύπτει ο ισχυρισμός.

Ορισμός 7.20
Αντικατάσταση *(substitution) σε ένα αλφάβητο* Σ *είναι μια οποιαδήποτε αντιστοίχιση των γραμμάτων του αλφαβήτου σε γλώσσες πάνω από το* Σ*, μια οποιαδήποτε συνάρτηση δηλ.*

$$f : \Sigma \to 2^{\Sigma^*},$$

μια συνάρτηση δηλ. που παίρνει τιμές τυχόντα υποσύνολα του Σ^*. Αν για κάθε $\alpha \in \Sigma$ η γλώσσα $f(a)$ είναι κανονική, τότε και η αντικατάσταση ονομάζεται κανονική.

Έχοντας μια αντικατάσταση $f : \Sigma \to 2^{\Sigma^*}$ μπορούμε να επεκτείνουμε το πεδίο ορισμού της από γράμματα του Σ σε λέξεις του Σ^*. Αν $w = \alpha_1 \cdots \alpha_n$, $\alpha_i \in \Sigma$, είναι μια λέξη, τότε ορίζουμε (χρησιμοποιούμε το ίδιο σύμβολο f για να συμβολίσουμε και την επεκτεταμένη συνάρτηση)

$$f(w) = f(\alpha_1) \cdots f(\alpha_n),$$

η γλώσσα δηλ. που προκύπτει από τη συγκόλληση των γλωσσών $f(\alpha_1), \ldots, f(\alpha_n)$.

Αν L είναι μια γλώσσα ορίζουμε ως συνήθως

$$f(L) = \bigcup_{w \in L} f(w).$$

Θεώρημα 7.4
Αν L κανονική, και η αντικατάσταση f είναι κανονική, τότε η $f(L)$ είναι κανονική γλώσσα.

Απόδειξη

(Σχέδιο απόδειξης.)

Αφού η L είναι κανονική τότε προκύπτει ως γλώσσα μιας κανονικής έκφρασης r. Είναι εύκολο να δούμε (αλλά δεν το κάνουμε με λεπτομέρεια εδώ) ότι η γλώσσα $f(L)$ είναι ακριβώς αυτή που προκύπτει αν τροποποιήσουμε την έκφραση r αντικαθιστώντας κάθε γράμμα α που εμφανίζεται στην r με μια κανονική έκφραση για τη γλώσσα $f(\alpha)$. Άρα η γλώσσα $f(L)$ δίδεται από κανονική έκφραση, άρα είναι κανονική.

■

✏ **7.32**
Αποδείξτε το Θεώρημα 7.4 ακολουθώντας τη «συνταγή» του σχεδίου απόδειξης που δόθηκε. Μπορείτε για παράδειγμα να χρησιμοποιήσετε επαγωγή ως προς το μήκος μιας κανονικής έκφρασης της κανονικής γλώσσας L.

Ορισμός 7.21
Μια αντικατάσταση f λέγεται ομομορφισμός *αν για κάθε $\alpha \in \Sigma$ η γλώσσα $f(\alpha)$ είναι μονοσύνολο.*

Επειδή κάθε πεπερασμένο σύνολο λέξεων είναι κανονική γλώσσα (από τον ορισμό του τι είναι κανονική γλώσσα) από το προηγούμενο θεώρημα έπεται ότι οι ομομορφισμοί διατηρούν την κανονικότητα των γλωσσών.

Ορισμός 7.22
Αν f είναι ομομορφισμός και L είναι μια γλώσσα, η αντίστροφη ομομορφική εικόνα *της L είναι η γλώσσα*

$$f^{-1}(L) = \{w \in \Sigma^* : \ f(w) \in L\}.$$

Θεώρημα 7.5
Αν f ομομορφισμός και L κανονική γλώσσα τότε και η $f^{-1}(L)$ είναι κανονική.

Απόδειξη

Έστω M ένα DFA που αναγνωρίζει την L. Φτιάχνουμε DFA M' ως εξής: κρατάμε ίδιες καταστάσεις και αρχικές και τελικές καταστάσεις με το M και ορίζουμε μόνο νέα συνάρτηση μετάβασης ως εξής: αν q είναι μια κατάσταση του M και $\alpha \in \Sigma$ ορίζουμε

$$\delta_{M'}(q, \alpha) = \delta_M(q, f(\alpha)).$$

Μεταβαίνουμε δηλ. στο M' σε εκείνη την κατάσταση όπου θα καταλήγαμε αν στο M ξεκινάγαμε από την κατάσταση q και ακολουθούσαμε τη *λέξη* $f(\alpha)$. Είναι φανερό ότι η λέξη w γίνεται αποδεκτή από το M' αν και μόνο αν η λέξη $f(w)$ γίνεται αποδεκτή από το M, άρα το DFA αναγνωρίζει τη γλώσσα $f^{-1}(L)$, οπότε αυτή είναι κανονική.
■

✏ **7.33**
Αν L είναι κανονική γλώσσα τότε και η γλώσσα

$$L^R = \left\{x \in \Sigma^* : \ x^R \in L\right\}$$

είναι κανονική. Με x^R συμβολίζουμε τη λέξη x με τα γράμματά της σε ανάποδη σειρά. Π.χ. $011^R = 110$.
Δουλέψτε πάνω σε μια κανονική έκφραση για την L.

7.10 Το Λήμμα Άντλησης και μη κανονικές γλώσσες

Υπάρχουν γλώσσες που δεν είναι κανονικές. Αυτό είναι προφανές για πολύ γενικούς λόγους, που δεν έχουν τόσο πολύ να κάνουν με τη φύση των κανονικών γλωσσών, παρά μόνο με το γεγονός ότι κάθε κανονική γλώσσα επιδέχεται μια *πεπερασμένη περιγραφή*. Αυτή μπορεί να είναι είτε μια κανονική έκφραση, είτε η δομή ενός DFA που την αναγνωρίζει, για παράδειγμα.

Πόσες όμως διαφορετικές πεπερασμένες περιγραφές υπάρχουν;

Είναι φανερό ότι αυτές είναι άπειρες σε πλήθος (αφού π.χ. υπάρχουν οσοδήποτε μεγάλες κανονικές εκφράσεις), αλλά αυτό δεν είναι επαρκής πληροφορία για το πλήθος τους. Είναι πολύ πιο ακριβές το ότι υπάρχουν *αριθμήσιμες* σε πλήθος πεπερασμένες περιγραφές, μπορούν δηλ. όλες οι πεπερασμένες περιγραφές να απαριθμηθούν: η περιγραφή 1, η περιγραφή 2, ..., η περιγραφή N, ..., με τρόπο ώστε να μη μείνει καμιά περιγραφή απ' έξω.

Το γιατί το σύνολο όλων των πεπερασμένων εκφράσεων (πάνω από ένα σταθερό αλφάβητο Σ) είναι αριθμήσιμο είναι απλό. Αφού το Σ είναι πεπερασμένο υπάρχουν πεπερασμένες σε πλήθος εκφράσεις που μπορούν να φτιάξουμε με μήκος n, για κάθε n. Για την ακρίβεια, υπάρχουν το πολύ $|\Sigma|^n$ τέτοιες εκφράσεις. Για να απαριθμήσουμε λοιπόν το σύνολο όλων των πεπερασμένων εκφράσεων, αριθμούμε πρώτα τις εκφράσεις μήκους 1, μετά αυτές μήκους 2, και συνεχίζουμε κατ' αυτόν τον τρόπο, ώστε δε μένει τίποτα αμέτρητο.

Είναι αρκετά πιο δύσκολο (και παραλείπουμε την απόδειξη) να δούμε ότι το σύνολο όλων των υποσυνόλων οποιουδήποτε άπειρου συνόλου *δεν είναι αριθμήσιμο*. Έτσι, το σύνολο όλων των γλωσσών πάνω από το Σ, δηλ. το σύνολο όλων των υποσυνόλων του άπειρου συνόλου Σ^* δεν είναι αριθμήσιμο. Άρα υπάρχει κάποια γλώσσα που δεν έχει αντίστοιχη πεπερασμένη περιγραφή, οπότε δεν είναι κανονική.

Το παραπάνω είναι ένα πολύ γενικό επιχείρημα, όπως είπαμε, και δεν εξαρτάται σχεδόν καθόλου από το τι εννοούμε κανονική γλώσσα, παρά μόνο ότι, ό,τι κι αν εννοούμε, η κανονική γλώσσα μπορεί να περιγραφεί πλήρως με μια πεπερασμένη ακολουθία από γράμματα, διαλεγμένα από ένα πεπερασμένο αλφάβητο. Με τον ίδιο τρόπο φαίνεται, π.χ. ότι υπάρχουν συναρτήσεις $f : \mathbb{N} \to \mathbb{N}$ που δεν είναι υπολογίσιμες από πρόγραμμα, ουσιαστικά ότι κι αν εννούμε με αυτό. Ας πούμε για παράδειγμα ότι θεωρούμε μια τέτοια συνάρτηση υπολογίσιμη αν υπάρχει ένα πρόγραμμα σε κάποια γλώσσα προγραμματισμού, ας πούμε την python που υπολογίζει τη συνάρτηση αυτή. Μα ένα πρόγραμμα αποτελεί πεπερασμένη περιγραφή της συνάρτησης, άρα, επειδή το πλήθος των συναρτήσεων $f : \mathbb{N} \to \mathbb{N}$ δεν είναι αριθμήσιμο, υπάρχει κάποια στην οποία δεν αντιστοιχεί πρόγραμμα, που δεν είναι δηλ. υπολογίσιμη.

Δε βοηθάει όμως αυτό το επιχείρημα στο να αποδείξει κανείς ότι συγκεκριμένες γλώσσες δεν είναι κανονικές. Αν και γνωρίζουμε δηλ. ότι οι περισσότερες γλώσσες (υπό την έννοια του πληθαρίθμου) δεν είναι κανονικές, είναι παρ' όλα αυτά δύσκολο να δείξουμε αυτό για μια συγκεκριμένη γλώσσα που μας δίδεται, π.χ. για την

$$L_1 = \{0^n 1^n : \ n = 0, 1, 2, \ldots\}.$$

Αυτή η γλώσσα απαρτίζεται από όλες τις λέξεις που έχουν αρχικά μια ομάδα από μηδενικά και μετά μια ίση σε μήκος ομάδα από άσους, και τίποτε άλλο. Θα δούμε σε λίγο ένα τρόπο απόδειξης του ότι η L_1 δεν είναι κανονική. Διαισθητικά όμως ο λόγος είναι ο εξής (το παρακάτω *δεν* αποτελεί απόδειξη): ένα αυτόματο είναι ουσιαστικά ισοδύναμο με ένα υπολογιστή σαν κι αυτούς που ξέρουμε με μόνο τον περιορισμό ότι ο υπολογιστής αυτός έχει πεπερασμένη και σταθερή μνήμη, δεν εξαρτάται δηλ. η ποσότητα της μνήμης του από το πρόβλημα που έχει να λύσει. Αν είχαμε ένα πρόγραμμα που τρέχει σε ένα τέτοιο υπολογιστή και το οποίο αναγνωρίζει τη γλώσσα L_1, αυτό το πρόγραμμα θα είχε πρόσβαση σε μνήμη της οποίας το μήκος δε μπορεί να εξαρτάται από το μήκος της λέξης προς αναγνώριση. Όμως, δε μπορούμε να φανταστούμε ένα πρόγραμμα (αλγόριθμο) που θα αποφασίζει αν μια λέξη ανήκει στην L_1 ή οχι χωρίς να «θυμάται» κάπου το πόσα μηδενικά έχει δει. Κι αυτό δε γίνεται αν ο αριθμός των μηδενικών είνάι πολύ μεγάλος, γιατί όσο αυξάνει το πλήθος των μηδενικών τόσο αυξάνει, χωρίς άνω φράγμα, το πλήθος των ψηφίων (η μνήμη) που χρειαζόμαστε για να αποθηκεύσουμε τον αριθμό αυτό.

Είναι δύσκολο να μετατρέψουμε το παραπάνω διαισθητικό επιχείρημα σε απόδειξη, οπότε η μέθοδος που ακολουθούμε για να δείξουμε ότι η L_1 δεν είναι κανονική είναι αρκετά διαφορετική. Χρησιμοποιούμε το ακόλουθο πολύ χρήσιμο λήμμα.

Θεώρημα 7.6
(Λήμμα Άντλησης – Pumping Lemma) Έστω ότι η L είναι κανονική. Τότε υπάρχει φυσικός αριθμός n (ο οποίος δε χρειάζεται να είναι μεγαλύτερος από τον ελάχιστο αριθμό καταστάσεων ενός DFA που αναγνωρίζει την L) ώστε για κάθε λέξη $z \in L$ με $|z| \geq n$, μπορούμε να γράψουμε

$$z = uvw, \;\; (u, v, w \in \Sigma^*, \; |v| \geq 1, |uv| \leq n),$$

ούτως ώστε για κάθε $i = 0, 1, 2, \ldots$, η λέξη $uv^iw \in L$ (αυτή είναι η λέξη που αρχίζει με u ακολουθείται από την v οποιοδήποτε πεπερασμένο αριθμό από φορές – ακόμη και 0–και τελειώνει με w).

Μια εναλλακτική μετάφραση του Pumping Lemma θα μπορούσε να είναι «Λήμμα Φουσκώματος». Είτε με τη μια είτε με την άλλη μετάφραση το Λήμμα Άντλησης χρησιμοποιείται για να παράγουμε (αντλούμε) νέες λέξεις μιας κανονικής γλώσσας από άλλες.

Απόδειξη

Έστω M ένα DFA με ελάχιστο αριθμό καταστάσεων που αναγνωρίζει τη γλώσσα L, και έστω n το πλήθος των καταστάσεων του M. Αν η λέξη z αναγνωρίζεται τότε ξεκινώντας από την αρχική κορυφή q_0 καταλήγουμε διαβάζοντας την z, με $|z| = m \geq n$, σε κάποια τελική κορυφή q_1 διανύοντας ένα μονοπάτι πάνω στο M:

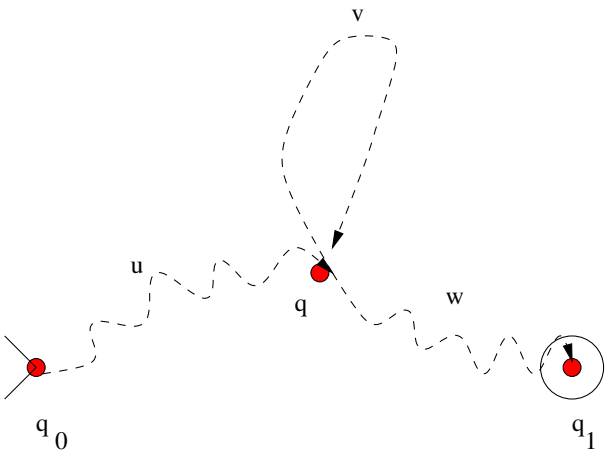
$$q_0 = q_{i_1} \to q_{i_2} \to \cdots \to q_{i_{m+1}} = q_1$$

όπου το πλήθος των ακμών είναι m (μια ακμή για κάθε γράμμα της z) και άρα το πλήθος των κορυφών είναι $m + 1 > n$. Συμπεραίνουμε ότι υπάρχουν κάποιες κορυφές που εμφανίζονται τουλάχιστον δύο φορές στο μονοπάτι. Από αυτές τις κορυφές ονομάζουμε q αυτή που πρωτοεμφανίζεται για δεύτερη φορά στο μονοπάτι και ονομάζουμε v τη λέξη που μεσολαβεί μέχρι την επόμενη εμφάνιση της q, ενώ u ονομάζομε το πρόθεμα της z μέχρι την πρώτη εμφάνιση της q και w ονομάζομε το επίθεμα της z μετά τη δεύτερη εμφάνιση της q (βλ. Σχήμα 7.17).

Είναι φανερό ότι $|v| \geq 1$ και ότι $|uv| \leq n$, αφού σίγουρα όταν θα έχουμε διαβάσει το n-οστό γράμμα της z θα έχουμε ήδη δεί τουλάχιστον μια κορυφή δύο φορές, και ανάμεσα σε αυτές που έχουμε δεί δύο φορές η πρώτη είναι εξ ορισμού η q. Επίσης είναι φανερό ότι το βρόχο που ξεκινά και τελειώνει στην q μπορούμε να μην το διανύσουμε καθόλου (οπότε δείχνουμε ότι η λέξη $uw \in L$) ή να τον διανύσουμε όσες φορές θέλουμε, ας πούμε i. Άρα η λέξη $uv^iw \in L$, όπως οφείλαμε να δείξουμε.

■

Πώς χρησιμοποιούμε το Λήμμα Άντλησης για να δείξουμε ότι η γλώσσα L_1 δεν είναι κανονική; Υποθέτουμε ότι είναι και καταλήγουμε σε άτοπο. Αν είναι λοιπόν, υπάρχει, από το Λήμμα Άντλησης, ένας φυσικός αριθμός n, τέτοις ώστε αν $z \in L_1$ και $|z| \geq n$ τότε ισχύουν τα συμπεράσματα του Λήμματος. Έχουμε $z = 0^n1^n \in L_1$ και $|z| \geq n$, άρα $z = uvw$, με $|uv| \leq n$ και μη κενό v, τέτοια ώστε για



Σχήμα 7.17: Το μονοπάτι που αντιστοιχεί στη λέξη uvw

κάθε $i = 0, 1, \ldots$ έχουμε $uv^i w \in L_1$. Αυτό όμως δε γίνεται μια και η λέξη $uv^2w = uvvw$ έχει σίγουρα περισσότερα 0 απ' ότι 1, αφού, λόγω του ότι $|uv| \leq n$, και το u και το v έχουν μόνο μηδενικά μέσα τους.

Ας δούμε τώρα άλλη μια εφαρμογή του λήμματος άντλησης σε παρόμοιο πρόβλημα. Για κάθε λέξη $x = \alpha_1 \cdots \alpha_n$, $\alpha_i \in \Sigma$, ορίζουμε την *αντεστραμμένη* λέξη $x^R = \alpha_n \cdots \alpha_1$, να είναι η x με αντεστραμμένη τη σειρά των γραμμάτων του. Ορίζουμε τη γλώσσα

$$L_2 = \{x \in (0+1)^* : \ x = x^R\},$$

να απαρτίζεται από όλες εκείνες τις λέξεις που διαβάζονται το ίδιο από αριστερά και από τα δεξιά.

Δείχνουμε τώρα ότι η L_2 δεν είναι κανονική. Έστω ότι είναι και έστω n ο φυσικός αριθμός του οποίου η ύπαρξη προκύπτει από το Λήμμα Άντλησης. Ορίζουμε τη λέξη $z = 1^n 01^n$ που είναι στην L_2. Γράφεται τότε η z ως $z = uvw$, με μη κενό v και $|uv| \leq n$, οπότε και οι λέξεις u, v έχουν μέσα μόνο 1, ώστε $uv^i w \in L_2$, για $i = 0, 1, 2, \ldots$. Αλλά προφανώς η λέξη $uw \notin L_2$ αφού αφαιρώντας το v αφαιρέσαμε κάποιους άσους από την αριστερή ομάδα άων αλλά όχι από τη δεξιά ομάδα, οπότε έχουμε καταλήξει σε άτοπο, άρα η L_2 δεν είναι κανονική.

✏ **7.34**
Δείξτε ότι η γλώσσα $\{xx : \ x \in \{0,1\}^*\}$ *δεν είναι κανονική.*

✏ **7.35**
Ποιες από τις παρακάτω γλώσσες του $(0+1)^*$ *είναι κανονικές;*

1. $\{0^{2n} : \ n \geq 1\}$
2. $\{0^m 1^n 0^{m+n} : \ m, n \geq 1\}$
3. *Οι λέξεις που δεν έχουν τρία διαδοχικά μηδενικά*
4. *Λέξεις με τόσα μηδενικά όσα και άσους.*
5. $\{xwx^R : \ x, w \in (0+1)^+\}$

Βιβλιογραφία Κεφαλαίου

[1] John E Hopcroft, Rajeev Motwani, and Jeffrey D Ullman. *Introduction to automata theory, languages, and computation*. Pearson, 2007.

Κεφάλαιο 8

Αλγόριθμοι για αυτόματα

Κύρια βιβλιογραφική αναφορά για αυτό το Κεφάλαιο είναι η Hopcroft, Motwani, and Ullman 2007.

8.1 Πότε ένα DFA αναγνωρίζει κενή ή άπειρη γλώσσα

Δοθέντος ενός DFA M καλούμαστε να αποφασίσουμε *με αλγοριθμικό τρόπο* για το αν

1. Υπάρχει έστω και μία λέξη που αναγνωρίζεται από το M,
2. Υπάρχουν άπειρες λέξεις που αναγνωρίζονται από το M.

Και στις δύο περιπτώσεις καλούμαστε να απαντήσουμε απλώς με ένα ναι ή όχι, και δε ζητούμε να βρούμε μία ή περισσότερες (πόσο μάλλον άπειρες) λέξεις για να αποδείξουμε τα λεγόμενά μας.

Πρέπει δηλ. να βρούμε ένα τρόπο να απαντήσουμε αν η γλώσσα του M είναι κενή ή όχι, και αν είναι άπειρη ή όχι ($L(M) = \emptyset$; και $|L(M)| = \infty$;). Και πρέπει ο τρόπος απόφασης να είναι αλγοριθμικός, δηλ. να μπορούμε να γράψουμε ένα πρόγραμμα στον υπολογιστή το οποίο, όποια και να είναι η απάντηση, να μπορεί να τη βρίσκει. Αυτό σημαίνει ότι σε κάθε περίπτωση (όποια και να είναι η απάντηση) πρέπει το πρόγραμμα αυτό (α) να τελειώσει και (β) να δώσει τη σωστή απάντηση.

Η απαίτηση για το (β) είναι προφανής στον περισσότερο κόσμο αλλά δεν είναι ίσως φανερό τι εννοούμε με το (α). Είναι λοιπόν χρήσιμο να τονίσουμε ότι ο ακόλουθος αλγόριθμος για να αποφασίσουμε το ερώτημα $L(M) = \emptyset$ δεν είναι αποδεκτός:

> Με τον υπολογιστή μας απαριθμούμε όλες τις λέξεις του Σ^* ως εξής. Πρώτα απαριθμούμε όλες τις λέξεις μήκους 0 (υπάρχει μόνο μία, η κενή λέξη ϵ), μετά απαριθμούμε τις λέξεις μήκους 1 (υπάρχουν τόσες όσα και α γράμματα του Σ, δηλ. το πλήθος τους είναι $|\Sigma|$), μετά τις λέξεις μήκους 2 (υπάρχουν ακριβώς $|\Sigma|^2$ τέτοιες), κ.ο.κ. Με αυτό τον τρόπο απαρίθμησης διανύουμε όλες τις λέξεις του Σ^*, χωρίς να ξεχνάμε καμιά. Για κάθε λέξη θα έρθει κάποτε η σειρά να την εξετάσουμε. *Παράλληλα* με την απαρίθμηση προγραμματίζουμε τον υπολογιστή μας να εξετάζει κάθε μια από τις αριθμούμενες λέξεις για το αν περνάνε από το M ή όχι. Αν έστω και μια βρεθεί που να αναγνωρίζεται από το M τότε σταματάει ο αλγόριθμος και απαντά ΝΑΙ (στο ερώτημα αν $L(M) = \emptyset$), αλλιώς συνεχίζει.

Είναι φανερό ότι αυτή η μέθοδος κάνει, κατά κάποιο τρόπο, μισή δουλειά, μια και δεν είναι ποτέ δυνατό να απαντήσει ΟΧΙ, αφού δεν ξέρουμε, όσες λέξεις και να έχουμε δει μέχρι στιγμής, για το αν υπάρχει λέξη της $L(M)$ που να βρίσκεται παρακάτω στην αρίθμησή μας, π.χ. να έχει μεγαλύτερο μήκος απ' ό,τι έχουμε εξετάσει μέχρι στιγμής. Αν η απάντηση στο ερώτημα είναι ΝΑΙ τότε, αργά ή γρήγορα, ο αλγόριθμός μας θα απαντήσει ΝΑΙ, δε συμβαίνει όμως το ίδιο και με το ΟΧΙ.

Πώς θα μπορούσε κάπως να διορθωθεί ο αλγόριθμος που μόλις περιγράψαμε;

Αν είχαμε ένα τρόπο, με δεδομένη την περιγραφή του M, να ξέρουμε πόσο μεγάλη (το πολύ) είναι η μικρότερη σε μήκος λέξη της $L(M)$, αν μια τέτοια λέξη υπάρχει, τότε θα προγραμματίζαμε τον υπολογιστή μας να σταματάει την απαρίθμηση όταν έχει περάσει αυτό το φράγμα και δεν έχει βρει ακόμη

λέξη της $L(M)$, αφού είναι πλέον σίγουρο ότι όσο και να συνεχίσει δε θα βρει άλλη. Αυτό το σκοπό, και για τα δύο ερωτήματα που μας απασχολούν, εξυπηρετεί το παρακάτω θεώρημα, που είναι ουσιαστικά πόρισμα του Λήμματος Άντλησης.

Θεώρημα 8.1
Αν M είναι ένα DFA με n καταστάσεις τότε

1. *$L(M) \neq \emptyset$ αν και μόνο αν υπάρχει $w \in L(M)$ με $|w| < n$.*
2. *$|L(M)| = \infty$ αν και μόνο αν υπάρχει $w \in L(M)$ με $n \leq |w| < 2n$.*

Απόδειξη

1. Αν υπάρχει $w \in L(M)$ με $|w| < n$ τότε προφανώς $L(M) \neq \emptyset$. Αντίστροφα, έστω $L(M) \neq \emptyset$ και $w \in L(M)$ έχει ελάχιστο μήκος. Αν $|w| \geq n$ τότε, από το Λήμμα Άντλησης, υπάρχει σπάσιμο $w = uvz$ με $v \neq \epsilon$ τέτοιο ώστε για κάθε $i \geq 0$ έχουμε $uv^iz \in L(M)$. Για $i = 0$ παίρνουμε $uz \in L(M)$, η οποία όμως λέξη έχει μήκος μικρότερο της $w = uvz$ η οποία είχε εξ αρχής υποτεθεί ότι έχει ελάχιστο μήκος, πράγμα άτοπο, άρα $|w| < n$.
2. Αν υπάρχει $w \in L(M)$ με $n \leq |w| < 2n$ τότε (χρησιμοποιώντας μόνο την ανισότητα $n \leq |w|$) από το Λήμμα Άντλησης το w σπάει σε $w = uvz$, $v \neq \epsilon$, έτσι ώστε οι λέξεις uv^iz, $i \geq 0$, ανήκουν όλες στην $L(M)$. Αλλά αυτές είναι άπειρες σε πλήθος, άρα $|L(M)| = \infty$. Αντίστροφα, έστω $|L(M)| = \infty$ και υποθέσουμε ότι δεν υπάρχει λέξη w με μήκος από n έως και $2n - 1$, ας πάρουμε w να είναι λέξη με ελάχιστο μήκος μεγαλύτερο ή ίσο του $2n$ (τέτοιες λέξεις υπάρχουν αναγκαστικά αφού η $L(M)$ έχει υποτεθεί άπειρη γλώσσα). Το Λήμμα Άντλησης εφαρμόζεται και πάλι αφού $|w| \geq 2n \geq n$ άρα η λέξη w γράφεται $w = uvz$, με $|uv| \leq n$ και $v \neq \epsilon$ και $uv^iz \in L(M)$ (για $i \geq 0$). Άρα $uz \in L(M)$ και αφού $|uvz| \geq 2n$ και $|v| \leq n$ συμπεραίνουμε ότι $|uz| \geq n$, άρα (έχουμε υποθέσει ότι δεν υπάρχουν λέξεις στην $L(M)$ με μήκος από n έως και $2n - 1$) $|uz| \geq 2n$, πράγμα που αντιφάσκει με το ότι η w έχει ελάχιστο μήκος ανάμεσα στις λέξεις της $L(M)$ με μήκος τουλάχιστον $2n$.
■

Είμαστε τώρα σε θέση να δείξουμε το ακόλουθο αποτέλεσμα.

Θεώρημα 8.2
Τα ακόλουθα ερωτήματα είναι αλγοριθμικά αποφασίσιμα:

1. *Αναγνωρίζει το DFA M μια μη κενή γλώσσα;*
2. *Αναγνωρίζει το DFA M μια άπειρη γλώσσα;*
3. *Αναγνωρίζουν τα DFA M_1 και M_2 την ίδια γλώσσα;*

Απόδειξη

1. Απαριθμούμε όλες τις λέξεις μήκους μέχρι και $n - 1$ με γράμματα από το Σ (υπάρχουν ακριβώς $1 + |\Sigma| + |\Sigma|^2 + \cdots + |\Sigma|^{n-1}$ τέτοιες λέξεις) και τις ελέγχουμε όλες αν περνάνε από το αυτόματο M. Αν έστω και μια από αυτές αναγνωρίζεται τότε απαντάμε ΝΑΙ, αλλιώς απαντάμε ΟΧΙ. Η μέθοδος είναι σωστή με βάση το Θεώρημα 8.1.1.
2. Απαριθμούμε όλες τις λέξεις μήκους από n έως και $2n - 1$ με γράμματα από το Σ. Αν έστω και μια από αυτές αναγνωρίζεται τότε απαντάμε ΝΑΙ, αλλιώς απαντάμε ΟΧΙ. Η μέθοδος είναι σωστή με βάση το Θεώρημα 8.1.2.
3. Θέλουμε να απαντήσουμε στο ερώτημα

$$L(M_1) \neq L(M_2).$$

Η απάντηση σε αυτό είναι ΝΑΙ αν και μόνο αν η ακόλουθη γλώσσα είναι μη κενή

$$(L(M_1) \cap L(M_2)^c) \cup (L(M_1)^c \cap L(M_2)). \tag{8.1}$$

Μπορούμε όμως αλγοριθμικά να κατασκευάσουμε ένα DFA M που αναγνωρίζει ακριβώς αυτή τη γλώσσα, οπότε μετά χρησιμοποιούμε τον αλγόριθμο του σκέλους 1 αυτού του Θεωρήματος για να αποφασίσουμε αν η γλώσσα της (8.1) είναι κενή ή όχι. Το αυτόματο M κατασκευάζεται ως εξής. Παρατηρούμε ότι η (8.1) γράφεται

$$(L(M_1)^c \cup L(M_2))^c \cup (L(M_1) \cup L(M_2)^c)^c$$

και ότι αυτή η έκφραση χρησιμοποιεί μόνο ενώσεις και συμπληρώματα. Αν έχουμε ένα DFA N και θέλουμε να φτιάξουμε ένα DFA N' για τη συμπληρωματική γλώσσα τότε απλά αλλάζουμε τις τελικές καταστάσεις του N σε μη τελικές και τις μη τελικές σε τελικές. Για να φτιάξουμε ένα DFA για την ένωση δύο γλωσσών (των οποίων ξέρουμε κάποια DFA) φτιάχνουμε πρώτα ένα ϵ-NFA για αυτή την ένωση και το μετατρέπουμε στη συνέχεια σε DFA. Όλα αυτά γίνονται αλγοριθμικά.
■

8.2 Σχέσεις ισοδυναμίας για γλώσσες και αυτόματα. Θεώρημα Myhill–Nerode

Πάνω στο σύνολο Σ^* όλων των λέξεων ορίζονται φυσιολογικά οι εξής σχέσεις ισοδυναμίας

1. Αν $L \subseteq \Sigma^*$ είναι μια γλώσσα η σχέση R_L ορίζεται ως: $x \; R_L \; y$ αν και μόνο αν για κάθε $z \in \Sigma^*$ έχουμε
$$xz \in L \Leftrightarrow yz \in L,$$
δηλ. τα xz, yz είτε ανήκουν και τα δυο στην L είτε κανένα.

2. Αν M είναι ένα DFA τότε ορίζουμε $x \; R_M \; y$ αν και μόνο αν
$$\delta(q_0, x) = \delta(q_0, y),$$
όπου q_0 είναι η αρχική κατάσταση του M και $\delta(\cdot, \cdot)$ είναι η συνάρτηση μετάβασης του M. Ισχύει δηλ. $x \; R_M \; y$ αν και μόνο αν το αυτόματο M καταλήγει στην ίδια κορυφή αφού διαβάσει το x και αφού διαβάσει το y, ξεκινώντας πάντα από την αρχική του κορυφή.

✏ **8.1**
Δείξτε ότι οι σχέσεις R_L και R_M είναι σχέσεις ισοδυναμίας.

✏ **8.2**
Δείξτε ότι η γλώσσα L είναι ένωση κάποιων κλάσεων ισοδυναμίας της R_L (ανεξάρτητα από το αν είναι η L κανονική ή όχι). Κάθε R_L-κλάση δηλ. είτε περιέχεται πλήρως στην L είτε δεν περιέχει λέξεις της L.

Ορισμός 8.1
Δείκτης *μιας σχέσης ισοδυναμίας R λέγεται ο πληθάριθμος του συνόλου των κλάσεων ισοδυναμίας της R.*

✏ **8.3**
Δείξτε ότι ο δείκτης της R_M είναι πεπερασμένος και ίσος με το πλήθος των κορυφών του M που είναι προσπελάσιμες από την αρχική κορυφή q_0. Μια κορυφή v λέγεται προσπελάσιμη αν υπάρχει λέξη w τ.ώ. $\delta(q_0, w) = v$.

Ορισμός 8.2
Μια σχέση R ορισμένη πάνω στο Σ^* λέγεται δεξιά αναλλοίωτη *(right invariant) αν για κάθε $x, y, z \in \Sigma^*$ ισχύει*
$$x \; R \; y \Rightarrow xz \; R \; yz. \tag{8.2}$$

✏ **8.4**
Δείξτε ότι οι σχέσεις R_L και R_M που ορίσαμε παραπάνω είναι δεξιά αναλλοίωτες.

✏ **8.5**
Αν M είναι ένα DFA δείξτε ότι η γλώσσα $L(M)$ που αναγνωρίζει το M είναι μια ένωση κλάσεων ισοδυναμίας μιας σχέσης ισοδυναμίας με πεπερασμένο δείκτη.
Εξετάστε την R_M.

Θεώρημα 8.3
*(*Θεώρημα Myhill–Nerode*) Αν $L \subseteq \Sigma^*$ τα ακόλουθα είναι ισοδύναμα:*

1. *Η γλώσσα L είναι κανονική.*
2. *Η γλώσσα L είναι ένωση κάποιων κλάσεων ισοδυναμίας μιας δεξιά αναλλοίωτης σχέσης ισοδυναμίας R με πεπερασμένο δείκτη.*
3. *Η σχέση R_L έχει πεπερασμένο δείκτη.*

Απόδειξη

$1 \Rightarrow 2$
Αν η L είναι κανονική τότε αναγνωρίζεται από ένα DFA M και το ζητούμενο είναι η Άσκηση 8.5.
$2 \Rightarrow 3$
Έστω ότι η γλώσσα L είναι ένωση κλάσεων μιας σχέσης ισοδυναμίας R που έχει πεπερασμένο δείκτη $t < \infty$. Θα δείξουμε ότι ο δείκτης της R_L είναι το πολύ t, άρα πεπερασμένος.

Δείχνουμε κατ' αρχήν τη συνεπαγωγή $x\ R\ y \Rightarrow x\ R_L\ y$: Έστω $z \in \Sigma^*$, $xz \in L$ και $x\ R\ y$. Επειδή R δεξιά αναλλοίωτη έπεται $xz\ R\ yz$. Άρα το yz ανήκει στην ίδια R-κλάση με το xz. Αφού όμως $xz \in L$, και η L είναι ένωση κλάσεων της R, ολόκληρη η R-κλάση του xz περιέχεται στην L, άρα $yz \in L$. Δείξαμε δηλ. ότι $xz \in L \Rightarrow yz \in L$, και ακριβώς το ίδιο προκύπτει και η αντίστροφη συνεπαγωγή, άρα $x\ R_L\ y$, όπως θέλαμε να δείξουμε.

Η συνεπαγωγή που δείξαμε ($x\ R\ y \Rightarrow x\ R_L\ y$) σημαίνει ότι κάθε κλάση της R περιέχεται εξ ολοκλήρου σε *μια* κλάση της R_L. Πράγματι, έστω $x \in K$, όπου K μια R-κλάση, και έστω $x \in S$, όπου S η R_L-κλάση του x. Δείχνουμε τότε ότι $K \subseteq S$. Έστω λοιπόν $y \in K$. Αυτό σημαίνει $x\ R\ y$ άρα και $x\ R_L\ y$, οπότε $y \in S$.

Αφού κάθε R-κλάση περιέχεται σε μια R_L-κλάση λοιπόν δε μπορούν οι R_L-κλάσεις να είναι περισσότερες από τις R-κλάσεις, γιατι τότε θα υπήρχε κάποια R_L-κλάση που δε θα περιείχε καμιά R-κλάση και θα ήταν κενή, πράγμα που εξ ορισμού δε γίνεται.
$3 \Rightarrow 1$
Υποθέτουμε τώρα ότι η R_L έχει πεπερασμένο δείκτη και δείχνουμε ότι η L αναγνωρίζεται από κάποιο DFA M, άρα είναι κανονική. Αν $x \in \Sigma^*$ συμβολίζουμε με $[x]$ την R_L-κλάση ισοδυναμίας της λέξης x.

- Ως σύνολο καταστάσεων του αυτομάτου M παίρνουμε το σύνολο Q όλων των R_L-κλάσεων, που είναι πεπερασμένο από την υπόθεση.
- Ως αρχική κατάσταση παίρνουμε την κλάση $[\epsilon]$ της κενής λέξης.
- Τη συνάρτηση μετάβασης ορίζουμε ως εξής:

$$\delta([x], \alpha) = [x\alpha], \quad (\alpha \in \Sigma). \tag{8.3}$$

- Ως τελικές κορυφές παίρνουμε εκείνες τις κλάσεις της R_L που περιέχονται στην L (δες Άσκηση 8.2).

✏ **8.6**
Δείξτε ότι ο ορισμός (8.3) είναι «καλός». Αυτό σημαίνει ότι αν $K = [x] = [y]$ και εφαρμόσουμε τον (8.3) για να ορίσουμε την κορυφή $\delta(K, \alpha)$ τότε παίρνουμε το ίδιο αποτέλεσμα είτε χρησιμοποιήσουμε το στοιχείο x στον (8.3) είτε το y.

Επαναλαμβάνοντας τον ορισμό (8.3) (ή εφαρμόζοντας επαγωγή στο μήκος της λέξης $w \in \Sigma^*$) βλέπουμε ότι

$$\delta([x], w) = [xw],$$

άρα $\delta([\epsilon], w) = [\epsilon w] = [w]$ που είναι τελική κατάσταση του M αν και μόνο αν $w \in L$, άρα το M αναγνωρίζει ακριβώς τη γλώσσα L.
■

8.3 Ελαχιστοποίηση DFA

Το ερώτημα που μας απασχολεί εδώ είναι πώς, δοθέντος ενός DFA M, να βρούμε ένα άλλο DFA, έστω N, που να είναι *ισοδύναμο* με το M (δηλ. $L(M) = L(N)$ – αναγνωρίζουν την ίδια γλώσσα) και να έχει τον ελάχιστο αριθμό καταστάσεων.

Εξετάζοντας την απόδειξη του θεωρήματος Myhill-Nerode βλέπει κανείς εύκολα ότι υπάρχει ουσιαστικά ένα μοναδικό τέτοιο ελάχιστο DFA, και είναι αυτό που ως σύνολο καταστάσεών του έχει το σύνολο των κλάσεων ισοδυναμίας της δεξιά αναλλοίωτης σχέσης ισοδυναμίας R_L, με $L = L(M)$, και ως συνάρτηση μετάβασης τη συνάρτηση $\delta([x], \alpha) = [x\alpha]$ (δείτε την απόδειξη του Θεωρήματος Myhill-Nerode) όπου $[x]$ συμβολίζει την κλάση της λέξης $x \in \Sigma^*$ και $\alpha \in \Sigma$. Είδαμε επίσης στην απόδειξη του θεωρήματος Myhill-Nerode ότι οι κλάσεις της σχέσης R_M είναι υποσύνολα των κλάσεων της R_L, και αυτό σημαίνει ότι, όποιο και να είναι το DFA M, το ελάχιστο αυτόματο μπορεί να προκύψει από το M αν όλες οι κορυφές του M που είναι R_L ισοδύναμες *συμπτυχθούν* σε μία κορυφή, ώστε πλέον να μην υπάρχουν στο νέο αυτόματο δύο ή περισσότερες κορυφές, που η κλάσεις τους να είναι R_L ισοδύναμες.

Η μέθοδος ελαχιστοποίησης λοιπόν αποφασίζει για το ποιες θα είναι οι καταστάσεις του ελάχιστου DFA αφού βρεί, για κάθε ζεύγος κορυφών του M, αν οι καταστάσεις αυτές είναι μεταξύ τους R_L-ισοδύναμες. Οι καταστάσεις του ελάχιστου αυτομάτου θα είναι τα σύνολα R_L-ισοδυνάμων κορυφών του M. Για να υπολογίσουμε για κάθε ζεύγος κορυφών u και v του M αν είναι R_L-ισοδύναμες θεωρούμε κατ' αρχήν όλα τα ζεύγη κορυφών ισοδύναμα και αν προκύψει για ένα ζεύγος κορυφών ότι δεν είναι τότε μόνο τις χωρίζουμε.

Έτσι, θέλουμε να υπολογίσουμε μια συνάρτηση $f(u, v)$ όπου u και v είναι δύο οποιεσδήποτε διαφορετικές κορυφές του M, και θέλουμε η συνάρτηση αυτή να κάνει 1 αν οι u και v ΔΕΝ είναι ισοδύναμες και 0 αν είναι. Κατ' αρχήν λοιπόν δίνουμε τις αρχικές τιμές,

$$\forall u, v \in Q, u \neq v,\ f(u, v) = 0, \tag{8.4}$$

όπου Q το σύνολο των κορυφών του M.

Σύμφωνα με τον ορισμό της σχέσης ισοδυναμίας R_L δύο λέξεις x και y είναι μεταξύ τους R_L-ισοδύναμες αν όποια και να είναι η λέξη z είτε και οι δύο λέξεις xz, yz ανήκουν στην L είτε κι οι δύο δεν ανήκουν. Αμέσως αυτό μας δίνει (με επιλογή $z = \epsilon$) ότι αν $u \in F$ και $v \notin F$ τότε οι u και v δεν είναι ισοδύναμες. Αυτό μας δίνει το επόμενο βήμα του αλγορίθμου μας

$$\forall u \in F, v \notin F\ f(u, v) = 1. \tag{8.5}$$

Είναι επίσης φανερό από τον ορισμό της R_L ότι αν για τις κορυφές u και v γνωρίζουμε ήδη ότι δεν είναι ισοδύναμες, και για τις δύο κορυφές a και b υπάρχει μια λέξη σ τέτοια ώστε $u = \delta(a, \sigma)$ και $v = \delta(b, \sigma)$ τότε και οι a, b δεν είναι μεταξύ τους R_L-ισοδύναμες. Αυτή η παρατήρηση μας δίνει τον υπόλοιπο αλγόριθμο: Ορίζουμε κατ' αρχήν το σύνολο S από ζεύγη κορυφών να περιέχει όλα τα ζεύγη κορυφών (u, v) με $u \in F$, $v \notin F$, δηλ. όλα τα ζεύγη κορυφών για τα οποία γνωρίζουμε ότι τα μέλη τους δεν είναι ισοδύναμα. Έστω τώρα ένα νέο σύνολο από ζεύγη κορυφών T που αποτελείται από όλα τα ζεύγη κορυφών (a, b) για τα οποία ισχύει ακόμη $f(a, b) = 0$ (θεωρούνται δηλ. ακόμη ισοδύναμα) και για τα οποία υπάρχει ένα γράμμα $\sigma \in \Sigma$ τέτοιο ώστε το ζεύγος

$$(\delta(a, \sigma), \delta(b, \sigma)) \in S.$$

Αφού υπολογίσουμε το σύνολο αυτό T θέτουμε μετά $f(a,b) = 1$ για όλα τα $(a,b) \in T$, και τέλος αντιγράφουμε το T πάνω στο παλιό S, το οποίο και πετάμε, και συνεχίζουμε την ίδια διαδικασία (φτιάχνουμε ένα νέο T που προκύπτει από το νέο S, κ.ο.κ.), έως ότου το σύνολο T που φτιάξουμε να προκύψει κενό. Αυτό σηματοδοτεί ότι δεν έχουμε πλέον άλλη πληροφορία να αντλήσουμε και σταματάμε εδώ.

Αποδεικνύεται ότι ο αλγόριθμος αυτός δουλεύει, δηλ. όταν σταματήσει έχουμε $f(u,v) = 1$ ακριβώς για εκείνα τα ζεύγη κορυφών (u,v) με μη R_L-ισοδύναμα μέλη.

Η κατασκευή του ελάχιστου αυτομάτου γίνεται τώρα όπως στην απόδειξη του θεωρήματος Myhill-Nerode: βάζουμε από μιά κορυφή για κάθε ομάδα ισοδυνάμων κορυφών του M. Για να βρούμε που θα πάμε με το γράμμα α από μια τέτοια «υπερκορυφή» επιλέγουμε μια οποιαδήποτε M-κορυφή της υπερκορυφής αυτής και βλέπουμε που μας πάει το α αν ξεκινήσουμε από αυτή την κορυφή στο παλιό μας αυτόματο M. Η M-κορυφή όπου καταλήγουμε ανήκει σε μια υπερκορυφή του νέου μας υπό κατασκευή αυτομάτου και σε αυτή πρέπει να μεταβούμε. Μια υπερκορυφή θεωρείται τελική αν περιέχει κάποια τελική κορυφή του M (αναγκαστικά τότε θα περιέχει μόνο τελικές κορυφές του F) ενώ η αρχική υπερκορυφή είναι αυτή που περιέχει την αρχική κορυφή του M.

Βιβλιογραφία Κεφαλαίου

[1] John E Hopcroft, Rajeev Motwani, and Jeffrey D Ullman. *Introduction to automata theory, languages, and computation*. Pearson, 2007.

Κεφάλαιο 9

Context free γραμματικές και γλώσσες

Κύρια βιβλιογραφική αναφορά για αυτό το Κεφάλαιο είναι η Hopcroft, Motwani, and Ullman 2007.

9.1 Ένας τρόπος περιγραφής απλών αριθμητικών εκφράσεων

Ας υποθέσουμε ότι θέλουμε να ορίσουμε το τι σημαίνει σωστά δομημένη αριθμητική έκφραση. Για να κάνουμε τα πράγματα πιο απλά (χωρίς να χαθεί η ουσία) ας περιοριστούμε σε αριθμητικές εκφράσεις όπου οι μόνες πράξεις είναι η πρόσθεση (+) και ο πολλαπλασιασμός (*), και όπου ισχύουν οι συνηθισμένοι κανόνες για τις παρενθέσεις. Ας υποθέσουμε επίσης ότι οι βασικές ποσότητες που φτιάχνουν μια έκφραση συμβολίζονται όλες με το γράμμα x. Για παράδειγμα η έκφραση $x * (x + x) + x$ είναι μια σωστή έκφραση ενώ η $xx + *()$ δεν είναι.

Έχουμε δηλαδή ένα πολύ περιορισμένο αλφάβητο

$$\Sigma = \{+, *, (,), x\}$$

και προσπαθούμε να ορίσουμε τη γλώσσα των σωστών εκφράσεων, που είναι ένα κομμάτι του Σ^*.

Ένας γρήγορος και καθαρός τρόπος να τις ορίσουμε είναι να σκεφτούμε το πώς τις φτιάχνουμε: κολλάμε μαζί, με συγκεκριμένους κανόνες, μικρότερες εκφράσεις και φτιάχνουμε μεγαλύτερες. Δίνουμε έτσι τον εξής ορισμό.

Ορισμός 9.1
Η λέξη x είναι σωστή έκφραση. Επίσης αν οι λέξεις w και v είναι σωστές εκφράσεις, τότε σωστές εκφράσεις είναι επίσης και οι λέξεις (w), $w + v$, $w * v$. Τέλος, σωστές εκφράσεις είναι μόνο οι λέξεις που προκύπτουν από τους άνω κανόνες.

Έτσι η λέξη $x * (x + x) + x$ είναι σωστή έκφραση επειδή οι λέξεις x και $(x + x) + x$ είναι σωστές, και η δεύτερη είναι σωστή επειδή επειδή οι $(x + x)$ και x είναι σωστές και η πρώτη από αυτές είναι σωστή επειδή η $x + x$ είναι σωστή και, τέλος, αυτή είναι σωστή επειδή η x είναι σωστή.

Ορισμοί σαν τον παραπάνω (αλλά και αρκετά πιο περίπλοκοι) κωδικοποιούνται στις λεγόμενες context free γραμματικές. Πριν δώσουμε τον ακριβή ορισμό για αυτές ας πούμε ότι η context free γραμματική που αντιστοιχεί στον παραπάνω ορσιμό είναι η:

1. $S \to x$
2. $S \to (S)$
3. $S \to S + S$
4. $S \to S * S$

Με το σύμβολο S συμβολίζουμε μια «μεταβλητή» λέξη, η οποία μπορεί να αντικατασταθεί με το δεξί μέλος μιας από τις *παραγωγές* ($S \to \ldots$) από τις οποίες απαρτίζεται η γραμματική. Η λογική είναι ότι ξεκινάμε με τη λέξη S και εφαρμόζουμε σε αυτήν συνεχώς κάποιους από τους κανόνες παραγωγής μέχρι να πάρουμε τη λέξη που θέλουμε. Αν αυτό καταστεί εφικτό τότε, και μόνο τότε, η λέξη αυτή θα είναι στην context free γλώσσα που περιγράφεται από την άνω context free γραμματική.

Με την παρακάτω ακολουθία μετασχηματισμών προκύπτει π.χ. η λέξη $x * (x + x) + x$

$$\begin{array}{rcll} S & \to & S + S & \text{(κανόνας παραγωγής 3)} \\ & \to & S * S + S & \text{(κανόνας παραγωγής 4)} \\ & \to & S * (S) + S & \text{(κανόνας παραγωγής 2)} \\ & \to & S * (S + S) + S & \text{(κανόνας παραγωγής 3)} \\ & \to & x * (x + x) + x & \text{(κανόνας παραγωγής 1, τέσσερεις φορές)} \end{array}$$

Εύκολα βλέπει κανείς ότι με όποιο τρόπο και να χρησιμοποιήσουμε τους κανόνες παραγωγής δε μπορούμε να πάρουμε από την S τη λέξη $xx + *()$.

9.2 Ορισμός context free γραμματικών και των γλωσσών τους

Ορισμός 9.2
Μια context free γραμματική G πάνω από ένα αλφάβητο Σ (τα τερματικά σύμβολα*) είναι μια πεπερασμένη συλλογή από*

- μη τερματικά σύμβολα*, που συνήθως τα συμβολίζουμε με κεφαλαία λατινικά γράμματα, και που περιλαμβάνουν το διακεριμένο σύμβολο S (αρχικό μη τερματικό σύμβολο)*
- *κανόνες παραγωγής $X \to w$, όπου X είναι ένα μη τερματικό σύμβολο και w είναι μια λέξη από γράμματα του Σ και μη τερματικά σύμβολα (η w μπορεί να είναι και η κενή λέξη).*

Αν G είναι μια Context Free Grammar(CFG), Context Free Γραμματική, και w, v είναι δύο λέξεις από τερματικά ή μη τερματικά σύμβολα, τότε γράφουμε

$$w \overset{G}{\Rightarrow} v$$

αν με χρήση ενός κανόνα παραγωγής $X \to \alpha$ μπορεί να προκύψει η λέξη v από τη λέξη w. Αυτό σημαίνει ότι αντικαθιστούμε μια εμφάνιση του μη τερματικού συμβόλου X στη λέξη w με τη λέξη α (που απαρτίζεται από τερματικά και μη τερματικά σύμβολα) και με την αντικατάσταση αυτή προκύπτει η λέξη v.

Για παράδειγμα, αν G είναι η γραμματική που ορίσαμε παραπάνω τότε ισχύει

$$x + S \overset{G}{\Rightarrow} x + (S)$$

μια και από την αριστερή λέξη προκύπτει η δεξιά αν χρησιμοποιηθεί ο κανόνας 2.

Ορίζουμε επίσης

$$w \overset{G}{\underset{*}{\Rightarrow}} v$$

να σημαίνει ότι υπάρχει πεπερασμένη ακολουθία λέξεων $v_1, \ldots, v_n$ ώστε

$$w \overset{G}{\Rightarrow} v_1 \overset{G}{\Rightarrow} \cdots \overset{G}{\Rightarrow} v_n \overset{G}{\Rightarrow} v,$$

ότι δηλ. η λέξη v μπορεί να προκύψει από τη λέξη w με επανειλημμένη χρήση των κανόνων παραγωγής της G. Στην παραπάνω γραμματική για τις εκφράσεις ισχύει, για παράδειγμα,

$$S \overset{G}{\underset{*}{\Rightarrow}} (S + S)$$

αφού μπορούμε από τη λέξη S να πάμε στη λέξη $(S + S)$ εφαρμόζοντας πρώτα τον κανόνα 3 και μετά τον κανόνα 2.

Έχοντας στα χέρια μας τον συμβολισμό αυτό μπορούμε εύκολα να ορίσουμε πλέον ποια είναι η *γλώσσα* που αντιστοιχεί σε μια λέξη (από τερματικά ή μη σύμβολα).

Ορισμός 9.3
Αν G είναι μια CFG και w μια λέξη από τερματικά ή μη τερματικά σύμβολα της G τότε η γλώσσα της w ορίζεται ως

$$L(w) = L_G(w) = \left\{x \in \Sigma^* : \ w \underset{*}{\overset{G}{\Rightarrow}} x\right\}.$$

Απαρτίζεται δηλ. η $L(w)$ από εκείνες τις λέξεις *χωρίς μη τερματικά σύμβολα* που μπορούν να παραχθούν σε πεπερασμένο πλήθος βημάτων από τη λέξη w με τους κανόνες παραγωγής της G.

Τέλος ορίζουμε *την* γλώσσα της G.

Ορισμός 9.4
Αν G είναι μια CFG η γλώσσα $L(G)$ ορίζεται να είναι η γλώσσα $L(S)$. Μια γλώσσα L λέγεται Context Free Language (CFL), Context Free Γλώσσα, αν είναι η γλώσσα κάποιας context free γραμματικής.

Είναι δηλ. η γλώσσα της G όλες οι λέξεις του Σ^* που παράγονται από το αρχικό μη τερματικό σύμβολο S.

Θα χρησιμοποιούμε συνήθως τη συντομογραφία

$$X \to w_1|w_2|\ldots|w_n$$

για να υποδηλώσουμε μια ομάδα από κανόνες παραγωγής

$$X \to w_1,\ X \to w_2,\ \ldots, X \to w_n,$$

με το ίδιο αριστερό μέλος.

✏ **9.1**
Ποια είναι η γλώσσα της γραμματικής με κανόνες $S \to \epsilon \mid 0S0 \mid 1S1$;

✏ **9.2**
Δώστε μια CFG για τη γλώσσα $\{0^n1^n : \ n = 1, 2, \ldots\}$.

✏ **9.3**
Ανατρέξτε πίσω στον ορισμό του τι είναι κανονική έκφραση. Αν σταθεροποιήσουμε το αλφάβητο σε, ας πούμε, $\Sigma = \{a, b\}$, δώστε μια CFG για τη γλώσσα των κανονικών εκφράσεων πάνω από το Σ.

9.3 Ένα ενδιαφέρον παράδειγμα με πλήρη απόδειξη

Ας δούμε τώρα ένα παράδειγμα μιας CFG με παραπάνω από ένα μη τερματικό σύμβολο. Η γραμματική αυτή θα έχει ως γλώσσα της όλες τις λέξεις του $\{a, b\}^*$ που έχουν ίδιο πλήθος από a και b. Θυμίζουμε εδώ ότι αυτή η γλώσσα δεν είναι κανονική (αποδεικνύεται εύκολα αυτό με χρήση του Λήμματος Άντλησης (Θεώρημα 7.6)).

Η γραμματική G_1 είναι η ακόλουθη:

1. $S \to aB \mid bA \mid \epsilon$
2. $A \to aS \mid bAA$
3. $B \to aBB \mid bS$

Θεώρημα 9.1
Η γλώσσα $L(G_1)$ απαρτίζεται από εκείνες τις λέξεις του $\{a, b\}^*$ με ίδιο πλήθος από a και b.

Απόδειξη

Κατ' αρχήν τα μόνα τερματικά σύμβολα που εμφανίζονται στους κανόνες της G_1 είναι τα a και b, άρα η $L(G_1)$ είναι υποσύνολο του $\{a,b\}^*$.

Ας συμβολίζουμε για μια λέξη w του $\{a,b\}^*$ με $A(w)$ και $B(w)$ αντίστοιχα το πλήθος των a και b που περιέχει.

Πρέπει να δείξουμε ότι ισχύει $A(w) = B(w)$ αν και μόνο αν $S \overset{G_1}{\underset{*}{\Rightarrow}} w$. Αλλά αν προσπαθήσουμε να δείξουμε μόνο αυτό θα συναντήσουμε δυσκολίες. Παρ' ότι δείχνει αντιφατικό μας διευκολύνει το να δείξουμε παράλληλα και άλλες δύο προτάσεις. Έτσι θα δείξουμε με επαγωγή ως προς το μήκος της λέξης w τις εξής τρείς ισοδυναμίες.

1. $w \in L(S)$ αν και μόνο αν $A(w) = B(w)$.
2. $w \in L(A)$ αν και μόνο αν $A(w) = B(w) + 1$.
3. $w \in L(B)$ αν και μόνο αν $B(w) = A(w) + 1$.

Ο ρόλος δηλ. των μη τερματικών συμβόλων A και B στην G_1 είναι να παράγουν όλες τις λέξεις με ακριβώς ένα a παραπάνω (για το A) και ακριβώς ένα b παραπάνω (για το B).

Όπως είπαμε συμβολίζουμε με n το μήκος της λέξης w και κάνουμε επαγωγή ως προς n. Αν $n = 0$, τότε $w = \epsilon$ και w παράγεται από το S με τον τελευταίο κανόνα παραγωγής του S ενώ δεν παράγεται από τα A ή B, αφού όλοι οι κανόνες παραγωγής των A και B παράγουν μη κενές λέξεις. Βλέπουμε έτσι ότι ισχύουν και οι τρεις ισοδυναμίες για τη λέξη $w = \epsilon$, τη μοναδική λέξη με μήκος $n = 0$.

Υποθέτουμε τώρα επαγωγικά ότι ισχύουν και οι τρεις άνω ισοδυναμίες για κάθε λέξη w με $|w| \leq n-1$.

Έστω τώρα w μια λέξη με μήκος n. Αποδεικνύουμε την πρώτη ισοδυναμία: $w \in L(S) \iff A(w) = B(w)$.

$\underline{w \in L(S) \Longrightarrow A(w) = B(w)}$

Αφού $w \in L(S)$ υπάρχει μια ακολουθία παραγωγών της G_1 που αρχίζει από το S και καταλήγει στη w. Αν το πρώτο γράμμα της w είναι a τότε στην πρώτη παραγωγή αναγκαστικά χρησιμοποιείται ο κανόνας $S \to aB$. Αυτό συνεπάγεται ότι $w = ax$ όπου x είναι μια λέξη για την οποία ισχύει $x \in L(B)$, και $|x| \leq n-1$. Από την επαγωγική υπόθεση έπεται ότι $B(x) = A(x) + 1$ και συνεπώς $A(w) = B(w)$. Ομοίως, αν το πρώτο γράμμα της w είναι b τότε ο πρώτος κανόνας παραγωγής από το S στο w είναι αναγκαστικά ο $S \to bA$, άρα $w = by$, με $y \in L(A)$ και $|y| = n-1$. Από την επαγωγική υπόθεση $A(y) = B(y) + 1$ από το οποίο προκύπτει $A(w) = B(w)$.

$\underline{A(w) = B(w) \Longrightarrow w \in L(S)}$

Αν το πρώτο γράμμα της w είναι a τότε $w = ax$ με $A(x) = B(x) - 1$, και $|x| = n-1$. Από την επαγωγική υπόθεση προκύπτει ότι $x \in L(B)$, άρα υπάρχει τρόπος να παράγουμε το x από το μη τερματικό σύμβολο B. Αρχίζοντας τότε από το S, εφαρμόζουμε τον κανόνα παραγωγής $S \to aB$ και ακολούθως παράγουμε από το B το x. Συνολικά έχουμε παραγάγει έτσι το w από το S δείχνοντας σε αυτή την περίπτωση $w \in L(S)$. Ομοίως, αν το πρώτο γράμμα της w είναι το b τότε γράφεται $w = by$ με $|y| = n-1$ και $A(y) = B(y) + 1$, άρα, με την επαγωγική υπόθεση, ισχύει $y \in L(A)$. Για να παραγάγουμε λοιπόν τη w από το S ξεκινούμε εφαρμόζοντας τον κανόνα $S \to bA$, και ακολούθως παράγουμε από το A το y, παίρνοντας έτσι τελικά το w.

Εδώ έχουμε δείξει το επαγωγικό βήμα για την πρώτη ισοδυναμία.

Δείχνουμε τώρα το επαγωγγικό βήμα για την ισοδυναμία $w \in L(A) \iff A(w) = B(w) + 1$. Προσέξτε ότι εδώ υπάρχει ασυμμετρία στην απόδειξη όσον αφορά το ρόλο που παίζει το a και το b ως πρώτο γράμμα της λέξης w.

$\underline{w \in L(A) \Longrightarrow A(w) = B(w) + 1}$

Έστω ότι το πρώτο γράμμα της λέξης w είναι το a. Τότε αναγκαστικά η πρώτη παραγαγωγή από το A στο w είναι η $A \to aS$, οπότε $w = ax$ με $|x| = n-1$ και αναγκαστικά τότε το x πρέπει να είναι παραγόμενο από το S, άρα $x \in L(S)$ και από την επαγωγική υπόθεση $A(x) = B(x)$, από το οποίο προκύπτει ότι $A(w) = B(w) + 1$.

Αν το πρώτο γράμμα της w είναι το b τότε ο πρώτος κανόνας που εφαρμόζεται στην παραγωγή της w από το A είναι αναγκαστικά ο $A \to bAA$, οπότε έχουμε $w = bx_1x_2$ όπου $x_1, x_2 \in L(A)$, και, φυσικά, $|x_1|, |x_2| \leq n-1$. Από την επαγωγική υπόθεση τώρα προκύπτει ότι $A(x_1) = B(x_1) + 1$ και $A(x_2) = B(x_2) + 1$, από τα οποία προκύπτει φυσικά ότι $A(w) = B(w) + 1$.

$A(w) = B(w) + 1 \Longrightarrow w \in L(A)$

Αν το πρώτο γράμμα της w είναι το a τότε $w = ax$ με $A(x) = B(x)$, $|x| = n-1$, οπότε από την επαγωγική υπόθεση προκύπτει $x \in L(S)$. Παράγοντας τώρα από το A με τον κανόνα παραγωγής $A \to aS$ και συνεχίζοντας παράγοντας από το S το x, καταλήγουμε σε μια ακολουθία παραγωγής του w από το A, δηλ. $w \in L(A)$.

Αν το πρώτο γράμμα της w είναι το b τότε $w = bx$ με $|x| = n-1$ και $A(x) = B(x) + 2$. Ισχύει όμως το παρακάτω Λήμμα.

Λήμμα 9.1
Αν για μια λέξη $x \in \{a,b\}^*$ ισχύει $A(x) = B(x) + 2$ τότε το x σπάει ως $x = x_1x_2$ όπου $A(x_1) = B(x_1) + 1$ και $A(x_2) = B(x_2) + 1$.

✏ **9.4**
Δείξτε το Λήμμα 9.1.

Οπότε η λέξη x σπάει σε δυο κομμάτια x_1 και x_2, $x = x_1x_2$, με μήκος το πολύ $n-2$ η καθε μία και με $A(x_i) = B(x_i) + 1$, $i = 1, 2$. Από την επαγωγική υπόθεση έχουμε τώρα $x_1, x_2 \in L(A)$. Για να παραγάγουμε λοιπόν από το A τη λέξη w αρχίζουμε με τον κανόνα παραγωγής $A \to bAA$ και ακολούθως αναπτύσσουμε το πρώτο A σε x_1 και το δεύτερο σε x_2, πετυχαίνοντας έτσι συνολικά μια παραγωγή της w από το A.

Παραλείπουμε την απόδειξη του επαγωγικού βήματος για την τρίτη ισοδυναμία μια και αυτή είναι εντελώς παρόμοια με τη δεύτερη ισοδυναμία, με τους ρόλους των a, b και A, B εναλλαγμένους.
■

9.4 Οι κανονικές γλώσσες είναι και context free

Θεώρημα 9.2
Κάθε κανονική γλώσσα είναι και context free.

Το αντίστροφο φυσικά δεν ισχύει όπως δείχνουν πολλά από τα παραδείγματα που έχουμε δει ως τώρα, π.χ. η γλώσσα $\{0^n1^n : n = 1, 2, \ldots\}$.

Απόδειξη

Έστω L κανονική γλώσσα. Αυτό σημαίνει ότι υπάρχει μια κανονική έκφραση r για τη γλώσσα. Αρκεί να δείξουμε ότι κάθε κανονική έκφραση περιγράφει μια context free γλώσσα.

Αρχίζουμε από τις απλούστερες κανονικές εκφράσεις και το δείχνουμε σταδιακά για όλες. Κάνουμε δηλ. επαγωγή ως προς το μήκος της κανονικής έκφρασης. Αν η κανονική έκφραση r έχει μήκος 1, τότε είναι αναγκαστικά ένα γράμμα του $\Sigma = \{\alpha_1, \ldots, \alpha_k\}$, το σύμβολο ϵ ή το σύμβολο $\emptyset$ (ανατρέξτε πίσω στον Ορισμό 7.19). Αν είναι γράμμα του Σ δηλ. $r = \alpha_j$ για κάποιο $j \in \{1, \ldots, k\}$, τότε η γλώσσα $L(r)$ είναι το μονοσύνολο $\{\alpha_j\}$, το οποίο δίνεται από την CFG $S \to \alpha_j$. Αν $r = \epsilon$ τότε $L(r) = \{\epsilon\}$ που δίνεται από την CFG $S \to \epsilon$, και αν $r = \emptyset$ τότε $L(r) = \emptyset$ και αυτό το σύνολο δίνεται από τη CFG $S \to S$, που προφανώς δεν παράγει τίποτα.

Αν τώρα το μήκος της έκφρασης r είναι μεγαλύτερο του 1 τότε, με βάση τον ορισμό των κανονικών εκφράσεων, η r είναι της μορφής

- $r = (st)$, με s, t κανονικές εκφράσεις μικρότερου μήκους. Από την επαγωγική υπόθεση υπάρχουν context free γραμματικές G_1 και G_2 τέτοιες ώστε $L(G_1) = L(s)$ και $L(G_2) = L(t)$. Για να φτιάξουμε μια CFG για τη γλώσσα $L(r) = L(s)L(t)$ μετονομάζουμε κατ' αρχήν όλα τα μη τερματικά σύμβολα της G_1 και της G_2 ώστε να είναι διαφορετικά μεταξύ τους και διαφορετικά από S, και

ονομάζουμε τα δύο αρχικά μη τερματικά σύμβολα σε S_1 και S_2 για τις G_1 και G_2 αντίστοιχα. Η CFG για τη γλώσσα $L(r)$ έχει ως κανόνες όλους τους κανόνες της G_1 και της G_2 συν τον κανόνα $S \to S_1 S_2$, που είναι και ο μόνος κανόνας για το αρχικό μη τερματικό σύμβολο S.

- $r = (s + t)$. Όπως και πριν όλα μόνο που ο επιπλέον κανόνας της γραμματικής δεν είναι τώρα ο $S \to S_1 S_2$ αλλά οι δύο κανόνες $S \to S_1 \mid S_2$.

- $r = (s^*)$. Μετονομάζουμε το αρχικό μη τερματικό σύμβολο της CFG για το s σε S_1 (ή κάποιο άλλο όνομα αν αυτό υπάρχει ήδη στη γραμματική) και προσθέτουμε τον κανόνα $S \to \epsilon \mid S_1 S$.

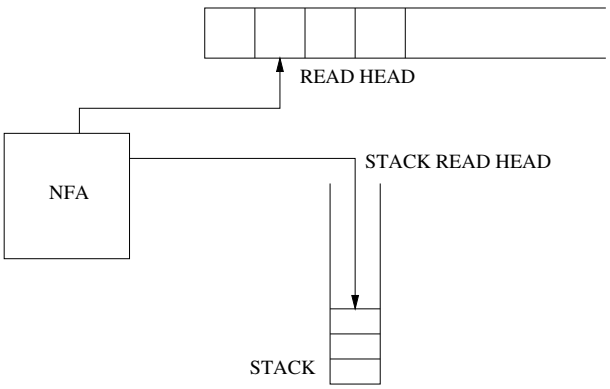
■

✏ **9.5**

Υπάρχει και άλλος τρόπος να δείξουμε ότι κάθε κανονική γλώσσα είναι κανονική. Μπορούμε να δουλέψουμε κατ' ευθείαν πάνω στο DFA ή NFA που αναγνωρίζει τη γλώσσα μας και να φτιάξουμε μέσω αυτού τη γραμματική. Διαλέξτε ένα από τα DFA ή NFA (η δουλειά είναι ουσιαστικά η ίδια) που εμφανίζονται σε αυτές τις σημειώσεις, π.χ. το αυτόματο που αναγνωρίζει τις λέξεις του $\{0, 1\}^*$ με περιττό πλήθος από μηδενικά και περιττό πλήθος από άσους (Σχήμα 7.1). Αντιστοιχήστε ένα μη τερματικό σύμβολο σε κάθε κατάσταση του αυτομάτου και βρείτε πώς πρέπει να φτιάξετε τους κανόνες παραγωγής ώστε να προκύψει μια CFG που να περιγράφει την ίδια γλώσσα. Διατυπώστε ένα γενικό τρόπο ώστε να πηγαίνετε από DFA ή NFA σε ισοδύναμη (που να περιγράφει την ίδια γλώσσα) CFG, χωρίς να περνάτε από την αντίστοιχη κανονική έκφραση.

9.5 Το αυτόματο με στοίβα (Push Down Automaton)

Όπως ακριβώς οι κανονικές γλώσσες έχουν αντίστοιχες μηχανές, τα DFA, ή τα NFA ή τα ϵ-NFA, που αναγνωρίζουν ακριβώς το σύνολο των κανονικών γλωσσών, έτσι υπάρχει και μια μηχανή, το αυτόματο με στοίβα, ή Push Down Automaton (PDA) που έχει την ιδότητα ότι μια γλώσσα L είναι context free αν και μόνο αν υπάρχει PDA που την αναγνωρίζει. Δε θα δείξουμε αυτή την ισοδυναμία εδώ (όπως είχαμε κάνει για τις κανονικές γλώσσες και τα πεπερασμένα αυτόματα).



Σχήμα 9.1: Ένα αυτόματο με στοίβα

Ένα PDA (Σχήμα 9.1) αποτελείται από τρία μέρη

1. Ένα NFA που το βλέπουμε σα «μονάδα ελέγχου» της μηχανής. Είναι σημαντικό εδώ να τονίσουμε ότι δε μπορούμε εδώ να αντικαταστήσουμε το NFA με DFA – τα αυτόματα με στοίβα είναι μη ντετερμινιστικές μηχανές.

2. Μια ταινία ανάγνωσης (read tape) που διαβάζεται από τον έλεγχο (NFA) με μια κεφαλή ανάγνωσης (read head) η οποία αρχίζει από τα αριστερά της ταινίας ανάγνωσης και κινείται μόνο προς τα δεξιά, και το πολύ κατά ένα σε κάθε βήμα (κύκλο) της μηχανής. Η προς αναγνώριση λέξη πρέπει να τοποθετηθεί εξ αρχής πάνω σε αυτή την ταινία από τον «χρήστη» της μηχανής.

3. Μια στοίβα (stack). Η στοίβα είναι μια απεριόριστη ποσότητα μνήμης την οποία όμως μπορούμε να διαχειριστούμε με πολύ περιορισμένο τρόπο. Φανταζόμαστε τη στοίβα σα μια (αρχικά κενή) στήλη από θέσεις μνήμης, που αρχίζει από το επίπεδό μας και εκτείνεται απείρως προς τα πάνω. Σε κάθε θέση μνήμης μπορούμε να γράψουμε ένα οποιοδήποτε από τα γράμματα του αλφαβήτου μας ή ένα πεπερασμένο αριθμό από άλλα ειδικά σύμβολα που ενδεχομένως μας διευκολύνουν στον «προγραμματισμό» του PDA. Στη στήλη αυτή μπορούμε να κάνουμε τις εξής τρεις πράξεις μόνο:

   - Μπορούμε να δούμε τα περιεχόμενα της πρώτης (από πάνω προς τα κάτω) θέσης μνήμης που είναι μη κενή. Αν η στοίβα είναι κενή μπορούμε να το διαπιστώσουμε αυτό.
   - Μπορούμε να προσθέσουμε κάτι στη στοίβα αλλά μόνο ακριβώς στη θέση μνήμης πάνω από την πρώτη (από πάνω προς τα κάτω) γεμάτη θέση μνήμης. Η πράξη αυτή αυξάνει λοιπόν το ύψος της στοίβας κατά 1.
   - Μπορούμε να διαγράψουμε την πιο πάνω θέση μνήμης (αν η στοίβα είναι κενή αυτή η πράξη δεν έχει κανένα αποτέλεσμα). Η πράξη αυτή ελαττώνει το ύψος της στοίβας κατά ένα αν η στοίβα δεν ήταν κενή.

Το NFA του αυτομάτου διαβάζει πάλι τα γράμματα της προς αναγνώριση λέξης ένα προς ένα, από αριστερά προς τα δεξιά, χωρίς και πάλι τη δυνατότητα να γυρίσει πίσω προς τα πίσω και να ξαναδιαβάσει την αρχή της λέξης. Και πάλι σε κάθε βήμα το NFA έχει τη δυνατότητα να εκτελέσει μια κίνηση ανάμεσα σε διάφορες δυνατές κινήσεις. Μια λέξη αναγνωρίζεται από το PDA αν κάποια επιλογή κινήσεων του NFA μπορεί να οδηγήσει σε αποδοχή της λέξης (το οποίο συμβαίνει αν στο τέλος το NFA είναι σε τελική κατάσταση).

Η σύνδεση του NFA με τη στοίβα γίνεται ως εξής: σε κάθε μετάβαση το NFA δεν επιλέγει το σύνολο των δυνατών επομένων καταστάσεων με κριτήριο μόνο το σε ποια κατάσταση βρίσκεται αυτό αλλά κοιτώντας ταυτόχρονα και ποιο είναι το περιεχόμενο της πάνω θέσης μνήμης της στοίβας (η μόνη θέση μνήμης που μπορεί άλλωστε να δει). Επίσης σε κάθε μετάβαση το NFA εκτελεί ενδεχομένως και μια από τις τρεις επιτρεπτές πράξεις στη στοίβα (διαβάζει την κορυφή της, προσθέτει κάτι στην κορυφή της, πετάει την πάνω θέση μνήμης χαμηλώνοντας την κορυφή της στοίβας κατά ένα, ή δεν κάνει τίποτα στη στοίβα).

Το μοντέλο του PDA είναι λειτουργικά ισοδύναμο με προγραμματισμό σε μια συνηθισμένη γλώσσα προγραμματισμού (π.χ. στην python) με τους εξής περιορισμούς και προσθήκες.

- Η μνήμη (εκτός της στοίβας) που χρησιμοποιεί το πρόγραμμά μας πρέπει να είναι συνολικά πεπερασμένη και γνωστή εξ' αρχής, ανεξάρτητα από το ποιο θα είναι το input (η προς αναγνώριση λέξη). Στην πράξη, αυτό το εξασφαλίζουμε δηλώνοντας μερικές μεταβλητές ακέραιου τύπου μόνο και λαμβάνοντας υπόψιν ότι κάθε τέτοια μεταβλητή δε μπορεί να μεγαλώσει απεριόριστα, έχει δηλ. συγκεκριμένο αριθμό από bits (δυαδικά ψηφία) που αντιστοιχούν σε αυτή.

- Η πρόσβαση στο input γίνεται μέσω της συνάρτησης `INP()` η οποία κάθε φορά που καλείται επιστρέφει και το επόμενο γράμμα της λέξης που εξετάζουμε. Όταν έχει διαβάσει όλα τα γράμματα επιστρέφει από κει και πέρα την ειδική τιμή -1.

- Υπάρχουν ακόμη άλλες τρεις «συναρτήσεις βιβλιοθήκης» με τις οποίες γίνεται ο χειρισμός της στοίβας, και μια συνάρτηση ακόμη με την οποία μπαίνει μέσα στη γλώσσα ο μη ντετερμινισμός που είναι απαραίτητος στο PDA. Οι συναρτήσεις για τη στοίβα είναι οι εξής:

`READ()`	Επιστρέφει τα περιεχόμενα της πάνω θέσης μνήμης της στοίβας ή -1 αν η στοίβα είναι άδεια.
`POP()`	αδειάζει μια θέση μνήμης από τη στοίβα ή δεν κάνει τίποτα αν η στοίβα είναι ήδη άδεια
`PUSH(x)`	Γράφει τον αριθμό `x` στην κορυφή της στοίβας, σε μια νέα θέση μνήμης

- Η συνάρτηση `NF` μέσω της οποίας κωδικοποιείται η μη ντετερμινιστική συμπεριφορά περιγράφεται στην επόμενη παράγραφο.

Μη ντετερμινιστικά «προγράμματα»

Γενικά ο μηχανισμός του μη ντετερμινισμού χρησιμοποιείται σε προβλήματα αποφάσεων, σε ερωτήματα δηλαδή που φιλοδοξούμε να λύσουμε υπολογιστικά και τα οποία επιδέχονται ΝΑΙ ή ΟΧΙ απάντηση, όπως ακριβώς είναι και το πρόβλημα που μας ενδιαφέρει εδώ, να αποφασίζουμε δηλ. αν μια λέξη που μας δίνεται ανήκει σε μια γλώσσα L ή όχι.

Η συνάρτηση μέσω της οποίας «υλοποιείται» ο μη ντετερμινισμός είναι η `NF(x)` η οποία επιστρέφει *μη ντετερμινιστικά* μια από τις επιλογές $0, 1, \ldots, x-1$. Το νόημα της συνάρτησης αυτής είναι ότι εμείς δεν έχουμε κανένα έλεγχο στο ποια από τις δυνατές επιλογές αυτή επιλέγει, αλλά πρέπει να γράψουμε το πρόγραμμά μας με τέτοιο τρόπο ώστε *αν αυτή η συνάρτηση επιστρέψει κατά τις κλήσεις της τις κατάλληλες επιλογές* τότε να κάνουμε τη λέξη δεκτή, αν αυτή είναι μέσα στη γλώσσα. Αλλά, δεν πρέπει να σε καμία περίπτωση να κάνουμε δεκτή μια λέξη που δεν ανήκει στη γλώσσα όποιες τιμές κι αν επιστρέψει η `NF`.

Για να γίνει κατανοητός ο τρόπος χρήσης της `NF` δείχνουμε παρακάτω μια συνάρτηση σε python η οποία παίρνει δύο ορίσματα `number` και `vector` και επιστρέφει `True` αν ο ακέραιος `number` περιέχεται στον πίνακα (λίστα) `vector` (ο οποίος έχει 1000 στοιχεία, τα `vector[0], …, vector[999]`) και `False` αν δεν περιέχεται.

```
def NumberInVector(number, vector):
        location = NF(1000)
        if number == vector[location]:
                return True
        else:
                return False
```

Πρέπει εδώ να ξεκαθαρίσουμε ότι η συνάρτηση `NumberInVector` λύνει το πρόβλημα που θέλουμε υπό την εξής έννοια:

- Αν ο αριθμός `number` είναι μέσα στον πίνακα `vector` τότε υπάρχει τρόπος να απαντήσει η `NF` ώστε ο αλγόριθμός μας να δώσει τη σωστή απάντηση, δηλ. `True`.

- Αν ο αριθμός `number` δεν είναι μέσα στον πίνακα `vector` τότε, ό,τι και να απαντήσει η `NF`, ο αλγόριθμός μας δεν υπάρχει περίπτωση να κάνει λάθος (αφού ελέγχει αν όντως βρίσκεται ο `number` στη θέση `vector[location]` πριν απαντήσει) και απαντάει πάντα `False`.

Αν δεν είχαμε στη διάθεσή μας τη συνάρτηση `NF` θα είμασταν αναγκασμένοι, λίγο-πολύ, να κάνουμε χίλιους ελέγχους για να διαπιστώσουμε αν ο δεδομένος αριθμός είναι μέσα στον πίνακα ή όχι. Παρατηρήστε ότι τώρα δεν υπάρχει ανακύκλωση κανενός είδους μέσα στη συνάρτηση και ότι η απάντηση βρίσκεται σε σταθερό χρόνο! Ο αλγόριθμος της συνάρτησης `NumberInVector` «μαντεύει» τη θέση στην οποία βρίσκεται στο `vector` ο αριθμός και απλά ελέγχει μετά αν είναι όντως έτσι πριν απαντήσει `True` ή `False`, ώστε να αποφύγει να κάνει λάθος στην περίπτωση που ο αριθμός δεν είναι μέσα. Ο αλγόριθμος αυτός δηλ. δεν υπάρχει περίπτωση να απαντήσει `True` ενώ η σωστή απάντηση είναι `False`, αλλά μπορεί κάλλιστα να απαντήσει `False` όταν η σωστή απάντηση είναι `True`. Αυτή η ασυμμετρία είναι πολύ χαρακτηριστική στους μη ντετερμινιστικούς αλγορίθμους.

Πρέπει να είναι φανερό με αυτό το παράδειγμα, ότι μη ντετερμινιστικοί αλγόριθμοι δεν μπορούν να υλοποιηθούν. Είναι απλά ένα χρήσιμο θεωρητικό κατασκεύασμα.

9.6 Παραδείγματα PDA

Η γλώσσα $L_1 = \{0^n 1^n : n = 1, 2, \ldots\}$

Η γλώσσα $L_1 = \{0^n 1^n : n = 1, 2, \ldots\}$ είναι context free (η γραμματική είναι: $S \to \epsilon \mid 0S1$). Θα δώσουμε εδώ ένα PDA για τη γλώσσα αυτή. Ισοδύναμα, θα περιγράψουμε το PDA αυτό σα μια συνάρτηση σε python, σύμφωνα με αυτά που είπαμε στην προηγούμενη παράγραφο. Η συνάρτηση αυτή θα μπορεί να χρησιμοποιεί σταθερή σε μέγεθος μνήμη και θα έχει πρόσβαση στη στοίβα μέσω των συναρτήσεων `READ()`, `POP()`, `PUSH()` που ορίσαμε στην προηγούμενη παράγραφο. Τυγχάνει για τη γλώσσα αυτή να μη χρειάζεται ο μη ντετερμινισμός οπότε δε θα χρησιμοποιήσουμε τη συνάρτηση `NF()`.

Το πρόγραμμα-PDA φαίνεται παρακάτω. Η συνάρτηση `f` επιστρέφει `True` αν η λέξη (που τη διαβάζουμε με διαδοχικές κλήσεις στη συνάρτηση `INP()`) ανήκει στην L_1 και `False` αλλιώς. Η στρατηγική της συνάρτησης είναι η εξής. Όσο διαβάζουμε μηδενικά τα σπρώχνουμε πάνω στη στοίβα. Για κάθε άσο που διαβάζουμε πετάμε κάτι από την στοίβα. Επίσης προσέχουμε ποτέ να μη διαβάσουμε 0 μετά που έχουμε διαβάσει κάποιο 1. Αν στο τέλος η στοίβα καταλήξει άδεια δεχόμαστε τη λέξη.

Ότι ακολουθεί το σύμβολο # αποτελεί σχόλιο και δεν είναι τμήμα του προγράμματος.

```
def f():
        SeenOne = False # Have not seen a 1 yet
        while True:
                letter = INP() # Read next letter
                if letter == 0:
                        if SeenOne:
                                return False # Reject after having seen a 1
                        PUSH(0) # Push 0s onto stack
                elif letter == 1:
                        SeenOne = True
                        if -1 == READ():
                                return False # The stack has emptied prematurely
                        POP() # For each 1 pop a 0 from stack
                else:
                        if -1 == READ():
                                return True # Accept if end of word and empty stack
                        else:
                                return False # Reject if stack not empty
```

Παρατηρήστε ότι, πέρα από τη στοίβα, το πρόγραμμα αυτό χρησιμοποιεί πεπερασμένη και προκαθορισμένη μνήμη. Για την ακρίβεια χρησιμοποιεί όλες κι όλες δύο μεταβλητές, τις `letter` (που χρησιμοποιείται για να κρατάει το επόμενο γράμμα ή -1) και `SeenOne` (που φροντίζουμε να είναι 0 όσο δεν έχουμε ακόμη δει άσο και μετά να είναι 1). Η μεταβλητή `letter` παίρνει τρεις διαφορετικές τιμές, αρκούν δηλ. 2 λογικά bits για να την αποθηκεύσουμε (μια και με αυτά κωδικοποιούμε 4 διαφορετικές τιμές), ενώ για τη μεταβλητή `SeenOne` που παίρνει δύο τιμές αρκεί ένα λογικό bit.

Μια σημαντική παρατήρηση εδώ είναι το παραπάνω PDA δε χρησιμοποιεί τη συνάρτηση `NF` και άρα πρόκειται για ένα ντετερμινιστικό πρόγραμμα (το NFA ελέγχου είναι στην πραγματικότητα DFA).

Η γλώσσα $L_2 = \left\{xx^R : x \in \{0,1\}^*\right\}$

Η γλώσσα $L_2 = \left\{xx^R : x \in \{0,1\}^*\right\}$ (x^R είναι η λέξη x γραμμένη ανάποδα) εύκολα φαίνεται ότι είναι context free. Μια CFG γι' αυτήν είναι απλούστατα η

$$S \to \epsilon \mid 0S0 \mid 1S1.$$

Παρακάτω δείχνουμε μια συνάρτηση `g()` η οποία υλοποιεί ένα PDA για την αναγνώριση της γλώσσας L_2. Εδώ χρησιμοποιείται η συνάρτηση `NF()`, πρόκειται δηλ. για ένα μη ντετερμινιστικό πρόγραμμα. Η στρατηγική είναι η εξής. Μέχρι τη μέση της ανάγνωσης της λέξης σπρώχνουμε τα γράμματα όπως τα διαβάζουμε πάνω στη στοίβα. Από τη μέση και πέρα για κάθε γράμμα που διαβάζουμε από το input πετάμε και ένα γράμμα από τη στοίβα και το συγκρίνουμε με αυτό που διαβάσαμε από το input. (Προσέξτε

ότι τα γράμματα θα πεταχτούν από τη στοίβα με αντίστροφη σειρά από αυτή με την οποία γράφτηκαν.) Αν είναι ίδια συνεχίζουμε (μέχρι να τελειώσει το input) αλλιώς απορρίπτουμε τη λέξη.

Η σημαντική παρατήρηση εδώ είναι ότι δεν μπορούμε να ξέρουμε πότε έχουμε φτάσει τη μέση της λέξης εισόδου! Αυτή τη βοήθεια αναλαμβάνει να μας δώσει η συνάρτηση `NF()`, η οποία μας λέει ακριβώς αυτό. Στο παρακάτω πρόγραμμα κάθε κλήση στην `NF()` κατά τη διάρκεια της εκτέλεσης του προγράμματος ισοδυναμεί με μια ερώτηση (στο Θεό, αν προτιμάτε) για το αν φτάσαμε τη μέση της λέξης ή όχι. Αν ο Θεός μας βοηθήσει με τη σωστή απάντηση θα δεχτούμε τη λέξη, μόνο όμως αν πρέπει να τη δεχτούμε. Δε μπορεί δηλ. να μας κοροϊδέψει με τρόπο ώστε να δεχτούμε μια λέξη ενώ δε θα έπρεπε (επαναλαμβάνουμε ότι είναι πολύ σημαντική αυτή η ασυμμετρία στα μη ντετερμινιστικά προγράμματα).

```
def g():
        mid = False # We have not reached the middle of the input yet
        while True:
                letter = INP() # Read next letter
                if not mid:
                        mid = (1 == NF(2)) # Is this letter after the middle;
                if not mid: # Have not passed the middle yet
                        if letter == -1:
                                return False # Premature end of input. Reject
                        PUSH(letter) # No, push letter onto stack
                        continue # Go back to while loop
                else: # We have passed the middle
                        top = READ() # Read top of stack
                        if (letter != -1) and (top == -1):
                                return False # Empty stack. Reject
                        POP() # Stack not empty. Pop top element.
                        if top != letter:
                                return False # Letters do not match. Reject.
                        continue # Letters do match. Keep going.
                if -1 == READ():
                        return True # Stack emptied with no problem. Accept.
```

Η γραμμή του παραπάνω προγράμματος όπου χρησιμοποιείται ο μη ντετερμινισμός είναι η `mid = (1 == NF(2))`, όπου (αν η μεταβλητή `mid` δεν έχει ήδη γίνει μια φορά `True`, οπότε και μένει για πάντα από κει και πέρα) θέτουμε τη μεταβλητή `mid` σε `False` ή `True` με μια κλήση στην `NF(2)`. Όταν η `NF(2)` επιστρέψει 1 θεωρούμε από κει και πέρα ότι έχουμε περάσει τη μέση, και προσπαθούμε με το πρόγραμμα να δούμε αν, με αυτή την υπόθεση μπορούμε να δεχτούμε τη λέξη.

Το πρόγραμμα αυτό χρησιμοποιεί τρεις μεταβλητές (`letter, mid, top`) κάθε μια από τις οποίες παίρνει τιμές μέσα στο σύνολο $\{0, 1, -1\}$ ή στο σύνολο `{True, False}` οπότε δύο λογικά bits αρκούν για την αποθήκευση κάθε μιας από αυτές.

9.7 Το Λήμμα Άντλησης για context free γλώσσες, και η εφαρμογή του

Όπως και στην περίπτωση των κανονικών γλωσσών υπάρχει και για τις context free γλώσσες, ένα «<Λήμμα Άντλησης» που είναι πολύ χρήσιμο στο να αποδεικνύουμε ότι ορισμένες γλώσσες δεν είναι context free. Η μορφή του είναι πολύ παρόμοια με το Λήμμα Άντλησης για κανονικές γλώσσες κα ο τρόπος χρήσης του επίσης.

Θεώρημα 9.3
(Λήμμα Άντλησης για context free γλώσσες) *Έστω ότι η γλώσσα L είναι context free. Τότε υπάρχει ένας φυσικός αριθμός n τέτοιος ώστε για κάθε λέξη $z \in L$ με $|z| \geq n$ να μπορούμε να γράψουμε*

$$z = uvwxy,$$

όπου

(α) $|vx| \geq 1$,

(β) $|vwx| \leq n$, *και*

(γ) για κάθε $i \geq 0$ *ισχύει* $uv^iwx^iy \in L$.

Δε θα δώσουμε απόδειξη του θεωρήματος αυτού, αλλά θα δούμε πώς χρησιμοποιείται για να δείξουμε ότι μια γλώσσα δεν είναι context free.

Παράδειγμα 9.1
Η γλώσσα $L_1 = \{a^nb^nc^n : n \geq 0\}$ **δεν είναι context free**

Ας υποθέσουμε ότι η L_1 *είναι context free. Έστω τότε* n *ο αριθμός που αναφέρεται στο Θεώρημα 9.3 και* $z = a^{2n}b^{2n}c^{2n} \in L_1$. *Από το Θεώρημα 9.3 η λέξη* z *γράφεται ως* $z = uvwxy$ *όπου ισχύουν τα συμπεράσματα του Θεωρήματος. Παρατηρούμε ότι η λέξη* vwx, *που σύμφωνα με το Θεώρημα έχει μήκος το πολύ* n, *δε μπορεί να περιέχει και* a *και* c, *ακριβώς επειδή το μήκος της δε φτάνει να «γεφυρώσει» τα* b *της λέξης* z. *Χωρίς βλάβη της γενικότητας υποθέτουμε ότι από τη λέξη αυτή λείπουν τα* a *(και το επιχείρημα είναι εντελώς παρόμοιο αν λείπουν τα* c*). Από το Θεώρημα 9.3 έπεται ότι η λέξη* $uwy \in L_1$ *(εφαρμόσαμε το Θεώρημα με* $i = 0$*). Αλλά για να πάμε από τη λέξη* z *στην* uwy *σβήσαμε το* u *και το* x, *τα οποία δεν έχουν* a *μέσα, άρα το πλήθος των* a *στη λέξη* uwy *έχει παραμείνει* $2n$. *Το μήκος της* uwy *όμως είναι αυστηρά μικρότερο του* $6n$ *(εδώ χρησιμοποιούμε το (α) από τα συμπεράσματα του Θεωρήματος), άρα δε μπορεί η λέξη* uwy *να ανήκει στην* L_1, *όπως είχαμε υποθέσει. Άρα η* L_1 *δεν είναι context free.*

✏ **9.6**
Δείξτε ότι η γλώσσα $\{xx : x \in \{0,1\}^*\}$ *δεν είναι context free.*

✏ **9.7**
Δείξτε ότι η γλώσσα $\left\{(ab)^k(cd)^k : k \in \mathbb{N}\right\}$ *δεν είναι κανονική.*

Βιβλιογραφία Κεφαλαίου

[1] John E Hopcroft, Rajeev Motwani, and Jeffrey D Ullman. *Introduction to automata theory, languages, and computation*. Pearson, 2007.

Κεφάλαιο 10

Υπολογισιμότητα

Κύρια βιβλιογραφική αναφορά για αυτό το Κεφάλαιο είναι η Hopcroft, Motwani, and Ullman 2007.

10.1 Υπολογίσιμες συναρτήσεις και αναδρομικά σύνολα

Μέχρι στιγμής έχουμε δει ουσιαστικά δύο κατηγορίες γλωσσών: τις κανονικές (regular) γλώσσες και τις context free γλώσσες. Η πρώτη κατηγορία περιέχεται στη δεύτερη. Από τη μέχρι στιγμής παρουσίαση πρέπει να έχει φανεί καθαρά ότι για κάθε μια από τις δύο κατηγορίες υπάρχει και ένα αντίστοιχο υπολογιστικό μοντέλο: τα πεπερασμένα αυτόματα (ντετερμινιστικά ή μη) για τις κανονικές γλώσσες και τα αυτόματα με στοίβα (push-down automata) για τις context free γλωσσες. Η αντιστοιχία στην οποία αναφερθήκαμε είναι ότι μια γλώσσα είναι στην κατηγορία που εξετάζουμε (κανονική ή context-free) αν και μόνο αν υπάρχει μια *μηχανή* του αντίστοιχου τύπου (πεπερασμένο αυτόματο ή αυτόματο με στοίβα) που αναγνωρίζει τη γλώσσα αυτή.

Είδαμε ότι το να υπάρχει ένα DFA για μια γλώσσα L είναι ισοδύναμο με το μπορεί κανείς να γράψει ένα πρόγραμμα σε μια γλώσσα προγραμματισμού (ας πούμε σε python) που να αναγνωρίζει τις λέξεις της L (να επιστρέφει δηλ. το πρόγραμμα αυτό 1 αν η λέξη που του δώσαμε ανήκει στην L και 0 αλλιώς), το οποίο δε χρησιμοποιεί απεριόριστη μνήμη αλλά μνήμη μεγέθους σταθερού και προκαθορισμένου, το ίδιο για όλες τις λέξεις της L. Ισοδύναμα, μιλάμε για ένα πρόγραμμα σε python που χρησιμοποιεί ένα σταθερό αριθμό μεταβλητών (όχι πίνακες) η καθεμία από τις οποίες χρησιμοποιεί προκαθορισμένη μνήμη (π.χ. ακέραιοι των 32 bits – δυαδικών ψηφίων).

Αντίστοιχα, ένα *ντετερμινιστικό* αυτόματο με στοίβα είναι ακριβώς ένα πρόγραμμα σε python που χρησιμοποιεί μεν πεπερασμένη μνήμη μόνο, αλλά έχει και πρόσβαση σε μια άπειρη στοίβα με ένα περιορισμένο όμως τρόπο, που του επιτρέπει να διαβάζει και να τροποποιεί πάντα μόνο την κορυφή της στοίβας. Τα *ντετερμινιστικά* αυτόματα με στοίβα δεν αρκούν για να αναγνωρίσουν όλες τις context free γλώσσες όμως, αλλά μπορεί κανείς με λίγη προσοχή να δείξει ότι και τα *μη ντετερμιστικά* αυτόματα με στοίβα έχουν ισοδύναμα python προγράμματα.

Είναι πλέον φυσιολογικός ο ακόλουθος ορισμός.

Ορισμός 10.1
(Υπολογίσιμη συνάρτηση) *Έστω Σ ένα πεπερασμένο αλφάβητο. Μια συνάρτηση $f : \Sigma^* \to \Sigma^*$ λέγεται* υπολογίσιμη συνάρτηση *αν υπάρχει ένα python πρόγραμμα* `P` *που με είσοδο $x \in \Sigma^*$ επιστρέφει τη λέξη $f(x)$.*

Τονίζουμε εδώ ότι δε μας ενδιαφέρει πόσο χρόνο θα χρειαστεί να *τρέξει* αυτό το πρόγραμμα για να υπολογίσει την απάντησή του, αλλά απαιτούμε πάντα από αυτό να μας βρεί τη σωστή απάντηση.

Ας παρατηρήσουμε εδώ ότι δεν υπάρχει κάτι μαγικό που να μας επιβάλλει το Σ^* σα πεδίο ορισμού και πεδίο τιμών στον παραπάνω ορισμό. Στη θέση του θα μπορούσε k να είναι οποιοδήποτε σύνολο που τα στοιχεία του να μπορούν να παρασταθούν, με κάποιο τρόπο, στον υπολογιστή (ένα τέτοιο σύνολο *δεν* είναι το σύνολο $\mathbb{R}$ των πραγματικών αριθμών). Αυτό όμως σημαίνει ουσιαστικά ότι μπορούμε να

γράψουμε κάτω μια λέξη από 0 ή 1 που να αντστοιχεί μοναδικά σε ένα στοιχείο του συνόλου αυτού. Πολλές φορές βλέπει κανείς τον ορισμό της υπολογίσιμης συνάρτησης να δίνεται π.χ. για συναρτήσεις από τους φυσικούς αριθμούς στους φυσικούς. Εμείς με τον όρο υπολογίσιμη συνάρτηση θα καταλαβαίνουμε οποιαδήποτε απεικόνιση την οποία μπορούμε να υπολογίζουμε χρησιμοποιώντας ένα πρόγραμμα.

Για παράδειγμα οι παρακάτω συναρτήσεις είναι υπολογίσιμες αφού εύκολα βλέπει κανείς ότι υπάρχουν προγράμματα που τις υπολογίζουν.

$$x \to x+1 \quad (\mathbb{N} \to \mathbb{N}),$$

$$x \to x^2 \quad (\mathbb{N} \to \mathbb{N}).$$

Ορισμός 10.2
(Αναδρομικό σύνολο) *Έστω Σ ένα πεπερασμένο αλφάβητο. Ένα σύνολο $L \subseteq \Sigma^*$ λέγεται* αναδρομικό *αν η χαρακτηριστική του συνάρτηση*

$$\chi_L(x) = \mathbf{1}\,(x \in L)$$

(ισούται με 1 αν $x \in L$, αλλιώς ισούται με 0) είναι υπολογίσιμη.

Και πάλι τη θέση του Σ^* μπορεί να πάρει οποιοδήποτε σύνολο του οποίου τα στοιχεία μπορούν να παρασταθούν στον υπολογιστή, π.χ. το σύνολο $\mathbb{N}$ των φυσικών αριθμών. Ένα σύνολο λοιπόν λέγεται αναδρομικό αν μπορούμε να γράψουμε ένα πρόγραμμα που να αποφασίζει πότε ένα στοιχείο x ανήκει στο σύνολο ή όχι. Για παράδειγμα, το σύνολο των πρώτων αριθμών (εκείνοι οι φυσικοί αριθμοί που δεν έχουν κανένα φυσικό αριθμό ως διαιρέτη, εκτός από τον εαυτό τους και τη μονάδα) είναι ένα αναδρομικό σύνολο, αφού μπορούμε να γράψουμε ένα πρόγραμμα που να να αποφασίζει αν ένας δοσμένος φυσικός αριθμός είναι πρώτος ή όχι, εξετάζοντας κάθε μικρότερό του φυσικό αριθμό για το αν διαιρεί το δοσμένο φυσικό ή όχι. Αυτό σίγουρα δεν είναι το «καλύτερο» πρόγραμμα που μπορεί κανείς να γράψει για αυτό το σκοπό, αλλά πάντως δουλεύει.

Είναι τώρα φανερό ότι οι κανονικές και οι context free γλώσσες είναι αναδρομικά σύνολα, αφού υπάρχουν προγράμματα που τις «αποφασίζουν». Η ιεραρχία των γλωσσών που έχουμε μέχρι τώρα δεί λοιπόν είναι η

$$(\text{κανονικές γλώσσες}) \subset (\text{context free γλώσσες}) \subset (\text{αναδρομικές γλώσσες}).$$

Και οι δύο παραπάνω εγκλεισμοί είναι γνήσιοι, υπάρχει δηλ. context free γλώσσα που δεν είναι κανονική (π.χ. η γλώσσα των παλίνδρομων λέξεων xx^R πάνω από ένα αλφάβητο) και αναδρομική γλώσσα που δεν είναι context free. Ένα παράδειγμα για το τελευταίο αποτελεί η γλώσσα $\{a^n b^n c^n : n \in \mathbb{N}\}$. Γι' αυτήν έχουμε δει στην §9.7 ότι δεν είναι context free γλώσσα, ενώ είναι αρκετά απλό να γράψει κανείς ένα python πρόγραμμα που να αναγνωρίζει πότε μια λέξη είναι της μορφής $a^n b^n c^n$. Ένα τέτοιο πρόγραμμα απλά μετράει το πλήθος των a, b και c και ελέγχει ότι είναι ίδια, καθώς και ότι όλα τα b έρχονται μετά από όλα τα a κι όλα τα c μετά τα b.

Είναι σημαντικό να τονίσουμε εδώ ότι η μεταβλητή του python προγράμματος όπου κρατιέται, π.χ., το πλήθος των a, είναι μια μεταβλητή για την οποία χρειαζόμαστε απεριόριστη μνήμη. Δεν είναι δηλ. δυνατόν να προκαθορίσουμε ένα άνω όριο για το πλήθος αυτό. Και επειδή ο φυσικός αριθμός x χρειάζεται περίπου $\log_2 x$ δυαδικά ψηφία για να παρασταθεί στον υπολογιστή, κι επειδή η συνάρτηση $\log_2 x$ αυξάνει (αν και αργά) χωρίς όριο όταν $x \to \infty$, αυτό το python πρόγραμμα δεν χρησιμοποιεί σταθερή μνήμη (αν αυτό συνέβαινε τότε η γλώσσα αυτή θα ήταν κανονική, ενώ δεν είναι καν context free).

✏ **10.1**
Αν τα σύνολα $A, B \subseteq \mathbb{N}$ είναι αναδρομικά δείξτε ότι το ίδιο ισχύει και για τα σύνολα $A \cap B$, $A \cup B$, A^c.

10.2 Μη υπολογίσιμες συναρτήσεις

Είναι πολύ φυσιολογικό το ερώτημα αν υπάρχουν συναρτήσεις που να μην είναι υπολογίσιμες. Για να συγκεκριμενοποιήσουμε τα πράγματα, ένα φυσιολογικό ερώτημα είναι αν υπάρχει συνάρτηση $f : \mathbb{N} \to \mathbb{N}$ για την οποία να μη μπορούμε να γράψουμε ένα πρόγραμμα που να την υπολογίζει.

Θεώρημα 10.1
Υπάρχει συνάρτηση $f : \mathbb{N} \to \mathbb{N}$ για την οποία δεν υπάρχει πρόγραμμα που να την υπολογίζει.

Απόδειξη

Η πρώτη παρατήρηση που κάνουμε είναι ότι το σύνολο των υπολογισίμων συναρτήσεων είναι αριθμήσιμο, μπορεί δηλ. κάποιος να γράψει κάτω όλες τις υπολογίσιμες συναρτήσεις $\mathbb{N} \to \mathbb{N}$ σε μια ακολουθία

$$f_1, f_2, \ldots, f_n, \ldots$$

(δεν υποθέτουμε εδώ ότι $f_i \neq f_j$ για $i \neq j$, αλλά επιτρέπουμε τις επαναλήψεις στην λίστα αυτή όλων των υπολογισίμων συναρτήσεων). Αυτό είναι άμεση συνέπεια του ότι το σύνολο όλων των προγραμμάτων είναι αριθμήσιμο. Πράγματι, αν το υποθέσουμε αυτό ως γνωστό δεν έχουμε παρά να απαριθμήσουμε όλα τα προγράμματα και για κάθε ένα από αυτά γράφουμε κάτω ποια συνάρτηση υπολογίζει (αν υπολογίζει συνάρτηση, αλλιώς δε γράφουμε τίποτα). Κάθε υπολογίσιμη συνάρτηση θα εμφανιστεί τότε στη λίστα μια και κάποια στιγμή θα εξετάσουμε ένα από τα προγράμματα που την υπολογίζουν.

Γιατί είναι τώρα το σύνολο όλων των προγραμμάτων αριθμήσιμο; Απλούστατα, κάθε πρόγραμμα δεν είναι παρά μια, συνήθως μεγάλη, λέξη πάνω από ένα συγκεκριμένο αλφάβητο Σ. Για παράδειγμα, όλα τα προγράμματα σε python γράφονται στο αλφάβητο που χρησιμοποιούν οι σύγχρονοι υπολογιστές και που περιλαμβάνει όλα τα λατινικά γράμματα, μικρά και κεφαλαία, δίαφορα σημεία στίξης, αριθμητικούς και άλλους τελεστές, ψηφία, κλπ. Απαριθμούμε πρώτα λοιπόν όλες τις λέξεις μήκους 1, μετά όλες τις λέξεις μήκους 2, όλες τις λέξεις μήκους 3, κ.ο.κ., και για κάθε λέξη που παράγουμε την αναφέρουμε στη λίστα των προγραμμάτων, αν αυτή είναι πρόγραμμα (πληροί δηλ. τους συντακτικούς κανόνες της γλώσσας προγραμματισμού που χρησιμοποιούμε). Μπορούμε να το κάνουμε αυτό ακριβώς επειδή όλες οι λέξεις πάνω από το Σ μήκους k είναι φυσικά πεπερασμένες σε πλήθος, και άρα κάποια στιγμή τελειώνουμε την απαρίθμηση των λέξεων μήκους k και προχωράμε στην απαρίθμηση των λέξεων μήκους $k+1$. Κάθε πρόγραμμα λοιπόν θα εμφανιστεί στη λίστα μας κάποια στιγμή ανάλογα και με το ποιο είναι το μήκος του. Έχουμε λοιπόν μέχρι στιγμής δείξει ότι το πλήθος όλων των υπολογισίμων συναρτήσεων είναι αριθμήσιμο.

Η απόδειξη του θεωρήματος συμπληρώνεται από το ότι το πλήθος *όλων* των συναρτήσεων από το $\mathbb{N}$ στο $\mathbb{N}$ δεν είναι αριθμήσιμο, δε μπορούμε δηλ. να διατάξουμε όλες αυτές τις συναρτήσεις σε μια ακολουθία

$$g_1, g_2, \ldots, g_n, \ldots$$

Αν μπορούσαμε τότε ας κοιτάξουμε τη συνάρτηση

$$f(k) = g_k(k) + 1.$$

Αυτή είναι προφανώς μια συνάρτηση από το $\mathbb{N}$ στο $\mathbb{N}$ άρα, αφού υποθέσαμε ότι όλες οι συναρτήσεις αυτές βρίσκονται στη λίστα g_i, υπάρχει κάποιο $i \in \mathbb{N}$ τέτοιο ώστε $f(k) = g_i(k)$ για κάθε $k \in \mathbb{N}$. Αυτό σημαίνει $g_k(k)+1 = g_i(k)$. Διαλέγοντας $k = i$ παίρνουμε άτοπο. (Το παραπάνω επιχείρημα ονομάζεται «διαγώνιο επιχείρημα» και βρίσκεται «πίσω» από τις περισσότερες αποδείξεις μη αριθμησιμότητας ενός συνόλου.)
■

Στην παραπάνω απόδειξη δείξαμε ότι υπάρχουν μη υπολογίσιμες συναρτήσεις δείχνοντας ότι το σύνολο των υπολογισίμων συναρτήσεων είναι αριθμήσιμο ενώ, αντίθετα, το σύνολο όλων των συναρτήσεων δεν είναι, είναι αυτό που λέμε *υπεραριθμήσιμο* σύνολο. Άρα, δεν μπορούν τα δύο σύνολα να είναι ίσα.

Αυτός είναι ένας κλασικός τρόπος απόδειξης στα μαθηματικά, η «υπαρξιακή απόδειξη», που αν και είναι αρκετά εύκολος και αποδεικνύει αυτό που θέλουμε, δεν είναι τόσο ικανοποιητικός επειδή αποδεικνύεται η ύπαρξη ενός αντικειμένου με ορισμένες ιδιότητες, αλλά, συνήθως, δεν προσδιορίζεται με κάποιο τρόπο κάποιο τέτοιο αντικείμενο. Στην προκειμένη περίπτωση γνωρίζουμε πλέον, μετά την απόδειξη του Θεωρήματος 10.1, ότι υπάρχουν συναρτήσεις από τους φυσικούς στους φυσικούς που δεν

είναι υπολογίσιμες, αλλά δε γνωρίζουμε καμία συγκεκριμένη τέτοια συνάρτηση. Θα δούμε αργότερα συγκεκριμένα παραδείγματα που για το καθένα θα έχουμε και ιδιαίτερο τρόπο απόδειξης του ότι δεν είναι υπολογίσιμα.

✏ **10.2**
Δεν υπάρχει κάποιος ιδιαίτερος λόγος που στο Θεώρημα 10.1 αναφερόμαστε σε συναρτήσεις $\mathbb{N} \to \mathbb{N}$. Δείξτε, για παράδειγμα, ότι υπάρχουν συναρτήσεις $\mathbb{N} \to \{0,1\}$ και $\Sigma^* \to \Sigma^*$, που δεν είναι υπολογίσιμες (Σ είναι ένα πεπερασμένο αλφάβητο).

10.3 Το Halting Problem. Άλλα μη αποφασίσιμα προβλήματα στα Μαθηματικά.

Τα προγράμματα ως αριθμοί, και το αντίστροφο Για τη συζήτηση από δω και πέρα θα χρειαστούμε να βλέπουμε το τυχόν python πρόγραμμα ως ένα φυσικό αριθμό, και τον τυχόντα φυσικό αριθμό ως ένα python πρόγραμμα. Πώς γίνεται αυτό; Πολύ απλά, ένα python πρόγραμμα δεν είναι παρά ένα κομμάτι κειμένου, μια λέξη δηλ. πάνω από ένα συγκεκριμένο αλφάβητο. Το αλφάβητο που χρησιμοποιείται στους υπολογιστές σήμερα είναι το

$$\Sigma = \{b_7 b_6 \cdots b_1 b_0 : \ b_i \in \{0,1\}, i = 0, \ldots, 7\}.$$

Αυτές είναι όλες οι λέξεις (bytes) με οκτώ δυαδικά ψηφία (bits) η κάθε μία και πολλές φορές ταυτίζουμε το συγκεκριμένο αλφάβητο με τους αριθμούς $0, \ldots, 255$. Ένα πρόγραμμα P λοιπόν είναι μια λέξη

$$P = w_1 \cdots w_N, \quad w_i \in \Sigma$$

και δεν έχουμε παρά να αντικαταστήσουμε κάθε w_i με τα δυαδικά του ψηφία ώστε να γράψουμε το P σα μια δυαδική λέξη με $8N$ δυαδικά ψηφία

$$P = b_{8N-1} b_{8N-2} \cdots b_1 b_0$$

την οποία λέξη μπορούμε να ερμηνεύσουμε ως ένα φυσικό αριθμό, που τον συμβολίζουμε στο εξής ως $\alpha(P)$. Αντίστροφα, αν n είναι ένας φυσικός αριθμός τον γράφουμε στο δυαδικό σύστημα και συμπληρώνουμε με μηδενικά (από τα αριστερά) το πλήθος των ψηφίων του αν χρειάζεται ώστε να είναι πολλαπλάσιο του 8, έστω $8k$. Κάθε μια από τις k οκτάδες τώρα τη βλέπουμε σαν ένα στοιχείο του Σ και ο αριθμός μας γίνεται τώρα μια λέξη του Σ^*. Αν αυτή η λέξη είναι ένα συντακτικά σωστό πρόγραμμα σε python τότε ονομάζουμε αυτό το πρόγραμμα $\pi(n)$, αν όχι, θέτουμε $\pi(n)$ να είναι το πρόγραμμα `return True`. (Η επιλογή αυτού του τελευταίου προγράμματος είναι τελείως τυχαία. Θα μπορούσαμε αντί γι' αυτό να επιστρέφουμε οποιοδήποτε άλλο.)

Η απεικόνιση $P \to \alpha(P)$ είναι εύκολο να δεί κανείς ότι είναι ένα προς ένα (αλλά όχι επί, αφού δεν είναι όλοι οι αριθμοί κωδικοποιήσεις συντακτικά σωστών προγραμμάτων), και ότι η απεικόνιση $n \to \pi(n)$ δεν είναι ένα προς ένα, αφού μπορεί δύο προγράμματα να μοιάζουν διαφορετικά αλλά να κάνουν την ίδια δουλειά, να υπολογίζουν δηλαδή την ίδια συνάρτηση. Είναι επίσης σημαντικό το ότι και οι δύο απεικονίσεις είναι υπολογίσιμες. Το ότι η $\alpha(P)$ είναι υπολογίσιμη είναι φανερό, ενώ το μόνο λεπτό σημείο όσον αφορά την υπολογισιμότητα της $\pi(n)$ είναι στο κομμάτι όπου πρέπει να ελέγξουμε αν η λέξη του Σ^* που προκύπτει είναι συντακτικά σωστό python πρόγραμμα ή όχι. Το να αποδείξουμε ότι κάτι τέτοιο είναι υπολογστικά εφικτό σημαίνει ουσιαστικά να γράψουμε ένα πρόγραμμα που να αναγνωρίζει αν ένα κομμάτι κειμένου (μια λέξη του Σ^*) είναι ένα σωστό συντακτικά python πρόγραμμα ή όχι. Τέτοια προγράμματα όμως υπάρχουν και χρησιμοποιούνται ευρέως αφού αποτελούν το πρώτο τμήμα των compilers ή interpreters (μεταφραστών) που παίρνουν ένα πρόγραμμα σε python και παράγουν από αυτό ένα ισοδύναμο πρόγραμμα σε «γλώσσα μηχανής».

Προσομοίωση. Θα χρειαστούμε επίσης το εξής: Υπάρχει ένα πρόγραμμα $S(n, x, t)$ το οποίο (α) βρίσκει το πρόγραμμα $P = \pi(n)$ και (β) «Τρέχει» το πρόγραμμα $P(x)$ για τόσα βήματα όσα λέει ο αριθμός t ή επ άπειρον αν ο αριθμός t είναι αρνητικός. Αν και όταν το πρόγραμμα $P(x)$ τελειώσει το $S(n, x, t)$

επιστρέφει ότι επέστρεψε το $P(x)$. Δε θα δείξουμε την ύπαρξη αυτού του προγράμματος που προσομοιώνει άλλα προγράμματα, μια και τέτοια προγράμματα υπάρχουν και χρησιμοποιούνται ευρέως στον προγραμματισμό (π.χ. interpreters, debuggers, κλπ).

Είμαστε έτοιμοι τώρα να αναφερθούμε στο Halting problem (πρόβλημα τερματισμού). Αυτό ρωτάει απλά αν υπάρχει ένα πρόγραμμα που να μπορεί να αποφασίζει αν ένα τυχόν άλλο πρόγραμμα που εμείς του προσδιορίζουμε θα τερματίσει ή όχι.

Είναι φανερό ότι υπάρχουν προγράμματα που δεν τερματίζουν ποτέ, π.χ. το παρακάτω.

```
def P(x):
        while True:
                x = 1
        return 1
```

Ένα τέτοιο πρόγραμμα θα ήταν εξαιρετικά χρήσιμο αν υπήρχε. Φανταστείτε να έχετε ένα python interpreter ο οποίος όχι μόνο θα μετάφραζε το πρόγραμμά σας σε γλώσσα μηχανής αλλά θα μπορούσε και να σας πει εκ των προτέρων αν το πρόγραμμά σας θα έπεφτε σε άπειρο βρόχο (loop) ή όχι. Δυστυχώς όμως τέτοιο πρόγραμμα δεν υπάρχει.

Στο εξής, για τυχόν πρόγραμμα P, θα γράφουμε $P\downarrow$ αν το πρόγραμμα P τερματίζει και $P\uparrow$ αν το P τρέχει επ' άπειρον.

Θεώρημα 10.2
Η συνάρτηση

$$H(n,x)=\begin{cases}1 & \alpha\nu\ \ (\pi(n))(x)\downarrow\\ 0 & \alpha\nu\ \ (\pi(n))(x)\uparrow\end{cases}$$

δεν είναι υπολογίσιμη.

Απόδειξη

Ας υποθέσουμε ότι η συνάρτηση $H(n,x)$ είναι υπολογίσιμη και ας συμβολίσουμε με P το πρόγραμμα που την υπολογίζει. Φτιάχνουμε τώρα το πρόγραμμα $Q(x)$ που χρησιμοποιεί το P ως υποπρόγραμμα:

```
def Q(x):
        if P(x, x)==0:
                return 1
        else:
                while True:
                        x = 1 # This does nothing and runs forever
```

Το πρόγραμμα $Q(x)$ που ορίσαμε έχει την ιδιότητα ότι τερματίζει αν και μόνο αν το $(\pi(x))(x)$ δεν τερματίζει.

Ποια είναι η συμπεριφορά του προγράμματος $Q(\alpha(Q))$; Τερματίζει ή όχι; Σύμφωνα με τη προηγούμενη παρατήρηση τερματίζει αν και μόνο αν το πρόγραμμα $(\pi(\alpha(Q)))(\alpha(Q))$ δεν τερματίζει. Αλλά $\pi(\alpha(Q))=Q$, οπότε δείξαμε ότι το πρόγραμμα $Q(\alpha(Q))$ τερματίζει αν και μόνο αν δεν τερματίζει, πράγμα προφανώς αδύνατο. Το συμπέρασμα είναι ότι η συνάρτηση H δεν είναι υπολογίσιμη.
■

Έχουμε λοιπόν δείξει ότι η, πολύ φυσιολογική, συνάρτηση $H(n,x)$ που διακρίνει πότε το πρόγραμμα $\pi(n)$ τερματίζει με input x ή όχι δεν είναι υπολογίσιμη. Έχουμε λοιπόν τώρα μια απόδειξη του ότι υπάρχουν μη υπολογίσιμες συναρτήσεις που είναι αρκετά πιο συγκεκριμένη από την προηγούμενη υπαρξιακή απόδειξη του Θεωρήματος 10.1. Μπορεί βέβαια και πάλι να πει κανείς ότι η $H(x)$ δεν έχει ίσως και τόσο ενδιαφέρον από μαθηματική άποψη μια και είναι μια συνάρτηση «κομμένη και ραμμένη» στα μέτρα της Θεωρίας Υπολογισμών, και άρα όχι, ίσως, τόσο φυσιολογική.

Υπάρχουν όμως πολλά παραδείγματα αρκετά φυσιολογικών μαθηματικών προβλημάτων που δεν επιδέχονται λύση αλγοριθμική, προβλήματα που προυπήρχαν της Θεωρίας Υπολογισμών.

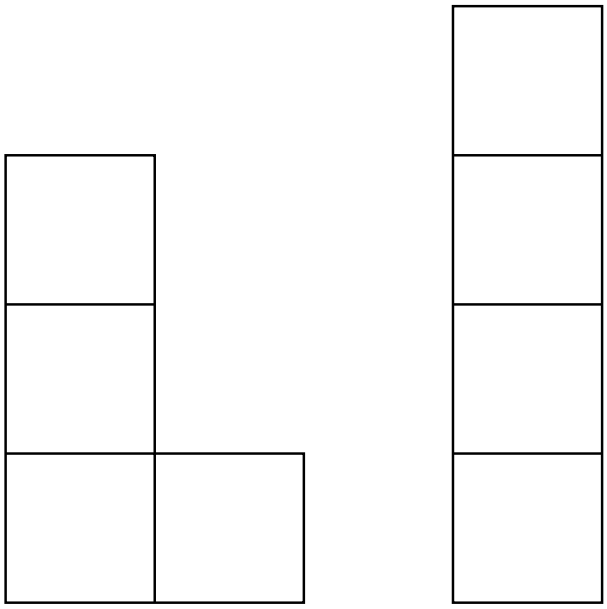
1. Δεν υπάρχει αλγόριθμος που να αποφασίζει αν ένα δοσμένο πολυώνυμο με ακεραίους συντελεστές (και οποιοδήποτε πλήθος από μεταβλητές)

$$P(x_1, \ldots, x_n) = \sum_{0 \le j_1, \ldots, j_n \le D} c_{j_1,\ldots,j_n} x_1^{j_1} \cdots x_n^{j_n}, \;\; c_{j_1,\ldots,j_n} \in \mathbb{Z},$$

έχει λύση (ρίζα) ανάμεσα στους ακεραίους, αν υπάρχουν δηλ. $x_1, \ldots, x_n \in \mathbb{Z}$ τ.ώ. $P(x_1, \ldots, x_n) = 0$.

2. Είναι ενδιαφέρον ότι αν ρωτήσουμε αν υπάρχει ρίζα πραγματική (και όχι αναγκαστικά ακέραια), αν δηλ. υπάρχουν $x_1, \ldots, x_n \in \mathbb{R}$ τ.ώ. $P(x_1, \ldots, x_n) = 0$, τότε υπάρχει αλγόριθμος που να απαντάει στο ερώτημα.

3. Ένα *πολυόμινο* είναι μια πεπερασμένη ένωση από μη αλληλοεπικαλυπτόμενα, μοναδιαία (πλευράς 1) τετράγωνα στο επίπεδο, τέτοια ώστε οι συντεταγμένες των κορυφών τους είναι ακέραιες. Στο Σχήμα 10.1 φαίνεται ένα σύνολο από δύο πολυόμινα. Ένα πολύ ενδιαφέρον ερώτημα είναι αν



Σχήμα 10.1: Ένα σύνολο από δύο πολυόμινα

ένα δεδομένο πεπερασμένο σύνολο από πολυόμινα μπορεί να χρησιμοποιηθεί για να «πλακοστρώσει» ολόκληρο το επίπεδο. Αυτό σημαίνει ότι καλύπτουμε το επίπεδο, χωρίς αλληλοεπικαλύψεις, από κομμάτια καθ' ένα από τα οποία είναι μια παράλληλη μεταφορά κάποιου από τα δεδομένα πολυόμινα. Για παράδειγμα, είναι σχετικά εύκολο να δει κανείς πως τα δύο πολυόμινα του Σχήματος 10.1 μπορούν να πλακοστρώσουν (αγγλικά: tiling) το επίπεδο, και είναι επίσης εύκολο να φτιάξει κανείς παραδείγματα απο σύνολο πολυομίνων που δε μπορούν, όπως και να μεταφερθούν, να πλακοστρώσουν το επίπεδο. Αποδεικνύεται λοιπόν ότι το να αποφασίσει κανείς αν ένα δεδομένο σύνολο από πολυόμινα μπορεί να πλακοστρώσει το επίπεδο είναι αλγοριθμικά ανεπίλυτο πρόβλημα. Δεν υπάρχει δηλ. πρόγραμμα που να του δίνουμε ένα τυχόν πεπερασμένο σύνολο από πολυόμινα και να μας απαντά αν επιδέχεται πλακόστρωση ή όχι.

10.4 Αναδρομικά απαριθμήσιμα (α.α.) σύνολα.

Ορισμός 10.3

(Αναδρομικά απαριθμήσιμο σύνολο) *Ένα μη κενό σύνολο $A \subseteq \mathbb{N}$ ονομάζεται* αναδρομικά απαριθμήσιμο *(α.α.) αν υπάρχει πρόγραμμα $P(x)$ που να απαριθμεί τα στοιχεία του A, δηλ. να έχουμε*

$$A = \{P(1), P(2), P(3), \ldots\},$$

με ενδεχόμενη επανάληψη των στοιχείων του A στο δεξί μέλος. Με άλλα λόγια, για κάθε $a \in A$ υπάρχει $n \in \mathbb{N}$, όχι κατ' ανάγκη μοναδικό, τέτοιο ώστε $a = P(n)$.

Παρατήρηση 10.1
Και πάλι, δεν υπάρχει, στον Ορισμό 10.3, τίποτα το μαγικό με το σύνολο $\mathbb{N}$ και θα μπορούσαμε στη θέση του να έχουμε, π.χ. το σύνολο Σ^*, όπου Σ ένα πεπερασμένο αλφάβητο.

Είναι σχεδόν άμεσο ότι κάθε αναδρομικό σύνολο είναι και α.α. Πράγματι, αν $\emptyset \neq A \subseteq \mathbb{N}$ είναι αναδρομικό τότε υπάρχει πρόγραμμα $Q(x)$ τέτοιο ώστε $Q(x) = 1 \Leftrightarrow x \in A$. Τότε το ακόλουθο πρόγραμμα απαριθμεί τα στοιχεία του A (m είναι, π.χ., το μικρότερο στοιχείο του A):

```
def P(x):
        if Q(x):
                return x
        else:
                return m
```

✏ **10.3**
Αν $A, B \subseteq \mathbb{N}$ είναι α.α. σύνολα δείξτε ότι το ίδιο ισχύει και για τα σύνολα $A \cap B$, $A \cup B$.

Από την άλλη μεριά είναι εύκολο να κατασκευάσουμε α.α. σύνολα που δεν είναι αναδρομικά. Για παράδειγμα, το σύνολο

$$A = \{x \in \mathbb{N} : \ \pi(x) \downarrow\}$$

δεν είναι αναδρομικό (αν ήταν τότε το πρόβλημα του τερματισμού θα ήταν υπολογίσιμο, ενώ έχουμε δείξει ότι δεν είναι) αλλά είναι α.α. Για να δούμε αυτό τον τελευταίο ισχυρισμό κάνουμε το εξής. Χρειαζόμαστε ένα πρόγραμμα που να απαριθμεί τα $x \in \mathbb{N}$ για τα οποία το πρόγραμμα $\pi(x)$ τερματίζει. Ισοδύναμα, φτιάχνουμε ένα πρόγραμμα που λειτουργεί επ' άπειρον και τυπώνει συνέχεια στην έξοδό του στοιχεία του A, χωρίς να παραλείψει κανένα. Το πρόγραμμα αυτό

- **Βήμα 1:** Πρώτα τρέχει (προσομοιώνει) το πρόγραμμα $\pi(1)$ για 1 βήμα.
- **Βήμα 2:** Έπειτα τρέχει (προσομοιώνει) τα προγράμματα $\pi(1), \pi(2)$ για 2 βήματα το καθένα
- ...
- **Βήμα k:** Τρέχει τα προγράμματα $\pi(1), \pi(2), \ldots, \pi(k)$ για k βήματα το καθένα,
- Συνεχίζει έτσι επ' άπειρον.

Στο τέλος του βήματος k το πρόγραμμά μας ελέγχει ποια από τα προγράμματα $\pi(1), \ldots, \pi(k)$ τελείωσαν μέσα στα πρώτα k τους βήματα, και τυπώνει τα αντίστοιχα x για αυτά που τελείωσαν στην έξοδό του. Είναι έτσι φανερό ότι κάθε x για το οποίο $\pi(x) \downarrow$ θα εμφανιστεί στην έξοδο του προγράμματός μας, και ότι σε αυτή την έξοδο εμφανίζονται μόνο τέτοια x (δηλ. στοιχεία του A). Αν $x \in A$ και το πρόγραμμα $\pi(x)$ τερματίζει μετά από t βήματα τότε ο αριθμός x εμφανίζεται για πρώτη φορά στην έξοδο του προγράμματός μας μετά το βήμα υπ' αριθμόν $\max\{x, t\}$, και εμφανίζεται και σε όλα τα μεταγενέστερα βήματα.

Έχουμε λοιπόν δείξει:

Θεώρημα 10.3
Κάθε αναδρομικό σύνολο είναι αναδρομικά απαριθμήσιμο αλλά το αντίστροφο δεν ισχύει.

Η ιεραρχία των γλωσσών τώρα γίνεται

(κανονικές γλώσσες) $\subset$ (context free γλώσσες) $\subset$ (αναδρομικές γλώσσες) $\subset$ (α.α. γλώσσες)

και όλοι οι εγκλεισμοί είναι γνήσιοι.

Η σχέση αναδρομικών και α.α. συνόλων φαίνεται πιο καθαρά στα επόμενα δύο θεωρήματα.

Θεώρημα 10.4
$A \subseteq \mathbb{N}$ είναι αναδρομικό αν και μόνο αν τα A, A^c είναι και τα δύο α.α.

Απόδειξη

Αν το A είναι αναδρομικό τότε αναδρομικό είναι και το A^c, άρα και τα δύο είναι α.α. Αντίστροφα τώρα, έστω ότι τα A, A^c είναι και τα δύο α.α., και ότι τα προγράμματα P και Q τα απαριθμούν, έχουμε δηλ.

$$A = \{P(1), P(2), \ldots\},\ A^c = \{Q(1), Q(2), \ldots\}.$$

Το παρακάτω πρόγραμμα $R(x)$, που χρησιμοποιεί τα P και Q ως υποπρογράμματα, επιστρέφει 1 αν $x \in A$ και 0 αλλιώς.

```
def R(x):
        i=1
        while True:
                if P(i) == x:
                        return 1
                if Q(i) == x:
                        return 0
                i = i+1
```

Το πρόγραμμα R απλούστατα παράγει όλους τους αριθμούς $P(1), Q(1), P(2), Q(2), \ldots$ και μόλις εμφανιστεί το x επιστρέφει 0 ή 1 ανάλογα με το αν το x εμφανίστηκε στην έξοδο του Q ή του P. Είναι σίγουρο ότι το x κάποτε θα εμφανιστεί (μια και είτε θα ανήκει στο A είτε στο A^c) και άρα για κάθε x το πρόγραμμα $R(x)$ τερματίζει.
■

Θεώρημα 10.5
Ένα σύνολο $A \subseteq \mathbb{N}$ είναι α.α. αν και μόνο αν υπάρχει πρόγραμμα $Q(x)$ τέτοιο ώστε

- *Αν $x \in A$ τότε $Q(x) = 1$, και*
- *Αν $x \notin A$ τότε $Q(x) = 0$ ή $Q(x) \uparrow$.*

Το πρόγραμμα Q στο θεώρημα λέει την αλήθεια για το αν $x \in A$, αν τελειώνει, μπορεί όμως και να τρέχει επ' άπειρον (αλλά αυτό μπορεί να συμβαίνει μόνο αν $x \in A$. Παρατηρήστε ότι υπάρχει ασυμμετρία στις δύο περιπτώσεις $x \in A$ και $x \notin A$, και αυτή η ασυμμετρία εκδηλώνεται και με το ότι υπάρχουν α.α. σύνολα που τα συμπληρώματά τους δεν είναι α.α.

Απόδειξη

Έστω ότι το πρόγραμμα P απαριθμεί τα στοιχεία του A:

$$A = \{P(1), P(2), \ldots\}.$$

Ορίζουμε το πρόγραμμα $Q(x)$ ως εξής:

```
def Q(x):
        i=1
        while True:
                if P(i)==x:
                        return 1
                i = i+1
```

Το πρόγραμμα $Q(x)$ επιστρέφει 1 αν και μόνο αν το x εμφανιστεί στη λίστα των τιμών του P, αλλιώς τρέχει επ' άπειρον.

Η άλλη κατεύθυνση του Θεωρήματος 10.5 αφήνεται ως άσκηση.

■

✏ **10.4**

Αποδείξτε την κατεύθυνση του Θεωρήματος 10.5 που λείπει από την απόδειξη που δόθηκε παραπάνω.

Βιβλιογραφία Κεφαλαίου

[1] John E Hopcroft, Rajeev Motwani, and Jeffrey D Ullman. *Introduction to automata theory, languages, and computation*. Pearson, 2007.

Κεφάλαιο 11

Εισαγωγή στη διακριτή πιθανότητα

Κύριες βιβλιογραφικές αναφορές για αυτό το Κεφάλαιο είναι οι Ross 1976, Grinstead and Snell 2012 και Hoel, Port, and Stone 1971.

11.1 Πειράματα

11.1.1 Ρίψη νομίσματος

Το πείραμα: Η ρίψη ενός νομίσματος.
Το αποτέλεσμα: Κορώνα (Κ) ή γράμματα (Γ)

Αν υποθέσουμε ότι επαναλαμβάνουμε το πείραμα N φορές τότε περιμένουμε τις μισές από αυτές *περίπου* το αποτέλεσμα να είναι Κ. Αυτή ακριβώς την έννοια κωδικοποιούμε λέγοντας ότι η πιθανότητα το πείραμα να έχει αποτέλεσμα Κ είναι ίση με 1/2. Η πιθανότητα p δηλ. να φέρει ένα πείραμα ένα αποτέλεσμα Α είναι η αναμενόμενη συχνότητα με την οποία θα εμφανιστεί το αποτέλεσμα Α αν επαναλάβουμε το πείραμα πάρα πολλές φορές. Αν δηλ. το επαναλάβουμε N φορές περιμένουμε το αποτέλεσμα Α να εμφανιστεί περίπου pN φορές. Εύλογο είναι ότι ο αριθμός p πρέπει να είναι ένας πραγματικός αριθμός στο διάστημα $[0, 1]$.

11.1.2 Ρίψη ζαριού

Το πείραμα: Η ρίψη ενός ζαριού.
Το αποτέλεσμα: Ένας από τους αριθμούς 1 έως 6.

Αν υποθέσουμε ότι επαναλαμβάνουμε το πείραμα N φορές τότε περιμένουμε το αποτέλεσμα να είναι ο αριθμός 2 με περίπου $N/6$ φορές. Η πιθανότητα δηλ. το αποτέλεσμα να είναι 2 ισούται με 1/6. Το ίδιο είναι και η πιθανότητα το αποτέλεσμα να είναι 1 ή 3 ή οποιοδήποτε άλλο από τα δυνατά αποτελέσματα.

Σε αυτό το παράδειγμα (ζάρι) όπως και στο προηγούμενο (νόμισμα) τα δυνατά αποτελέσματα είναι όλα ισοπίθανα.

Παρατηρήστε επίσης ότι αν αθροίσουμε (είτε στο παράδειγμα του νομίσματος είτε του ζαριού) τις πιθανότητες των δυνατών αποτελεσμάτων θα πάρουμε 1. Αυτό είναι αναμενόμενο με βάση την ερμηνεία που έχουμε προσδώσει στην πιθανότητα ως συχνότητα εμφάνισης του αποτελεσματος: αν επαναλάβουμε το πείραμα N φορές τότε το άθροισμα των συχνοτήτων εμφάνισης των αποτελεσμάτων είναι 1.

11.1.3 Ζεύγος νομισμάτων

Το πείραμα: Ρίχνουμε δύο νομίσματα και παρατηρούμε τι (Κ ή Γ) έφερε το κάθε νόμισμα.
Το αποτέλεσμα: Όλα τα ζεύγη (x, y) όπου τα x, y είναι Κ ή Γ.

Ερμηνεύοντας όπως και προηγουμένως την πιθανότητα ενός δυνατού αποτελέσματος ως τη συχνότητα με την οποία εμφανίζεται εύκολα καταλήγουμε ότι οι πιθανότητες των τεσσάρων δυνατών αποτελεσμάτων (Κ,Κ), (Κ,Γ), (Γ,Κ) και (Γ,Γ) πρέπει να είναι όλες ίσες και άρα ίσες με 1/4. Ένας άλλος τρόπος να το σκεφτούμε αυτό είναι να παρατηρήσουμε ότι αν εκτελέσουμε το πείραμα N φορές περιμένουμε

περίπου τις μισές από αυτές το πρώτο νόμισμα να έρθει Κ, και περίπου τις μισές από αυτές να έρθει και το δεύτερο νόμισμα Κ, αφού οι ρίψεις των δύο νομισμάτων δεν αλληλοεπηρεάζονται. Άρα η πιθανότητα του αποτελέσματος (Κ,Κ) πρέπει να είναι 1/4.

11.1.4 Αριθμός παιδιών

Το πείραμα: Ένα ζευγάρι κάνει συνεχώς παιδιά μέχρι να κάνει το πρώτο αγόρι, οπότε και σταματάει. Υποθέτουμε ότι σε όλες τις γέννες γεννιέται ένα παιδί κι ότι μπορούν να κάνουν απεριόριστα μεγάλο αριθμό παιδιών.
Το αποτέλεσμα: Ο αριθμός N, $N = 1, 2, 3, \ldots$, των παιδιών που κάνει τελικά το ζευγάρι.

Το σύνολο των δυνατών αποτελεσμάτων εδώ είναι άπειρο, αλλά αριθμήσιμο.

Η επίλυση του προβλήματος αυτού συνίσταται στο να υπολογιστεί η πιθανότητα να έχουμε $N = 1$, η πιθανότητα να έχουμε $N = 2$, κλπ. Για παράδειγμα, είναι πολύ εύκολο να δούμε ότι η πιθανότητα $N = 1$ ισούται με $1/2$ (υποθέτουμε εδώ ότι η πιθανότητα γέννησης αγοριού είναι 1/2), αφού $N = 1$ όταν και μόνο όταν το πρώτο παιδί που θα γεννηθεί είναι αγόρι. Θα δούμε αργότερα ότι η πιθανότητα να έχουμε $N = k$, για ένα οποιοδήποτε φυσικό αριθμό k, ισούται με 2^{-k}.

Αν το δεχτούμε αυτό τότε επαληθεύουμε εύκολα και πάλι ότι το άθροισμα των πιθανοτήτων για όλα τα δυνατά αποτελέσματα του πειράματος ισούται με 1:

$$\sum_{k=1}^{\infty} 2^{-k} = 1.$$

Για να δείτε την παραπάνω ισότητα χρησιμοποιήστε την ταυτότητα (άθροισμα άπειρης γεωμετρικής σειράς) για $z = 1/2$:

$$\sum_{k=0}^{\infty} z^k = 1 + z + z^2 + z^3 + \cdots = \frac{1}{1-z}, \tag{11.1}$$

που ισχύει για οποιοδήποτε μιγαδικό αριθμό z με $|z| < 1$ (Άσκηση 1.20.)

✏ **11.1**
Βρείτε ένα τύπο για το άθροισμα $\sum_{k=0}^{N-1} kz^k = z + 2z^2 + 3z^3 + \cdot + (N-1)z^{N-1}$.
Χρησιμοποιήστε την Άσκηση 1.20.

11.1.5 Χρόνος αναμονής

Το πείραμα: Καθόμαστε μπροστά από ένα κατάστημα και μετράμε το χρόνο που περνάει από τη στιγμή που θα μπεί ένας πελάτης μέχρι να μπεί ο επόμενος.
Το αποτέλεσμα: Ένας πραγματικός αριθμός $t \geq 0$.

Σε αντίθεση με τα παραδείγματα του ζαριού και του νομίσματος το πλήθος των δυνατών αποτελεσμάτων σε αυτό πείραμα είναι άπειρο και μάλιστα υπεραριθμήσιμο. Δεν έχει εδώ νόημα να αντιστοιχίσουμε μια πιθανότητα εμφάνισης σε κάθε δυνατό t. Εξάλλου είναι φανερό ότι αν επαναλάβουμε το πείραμα αυτό πολλές φορές είναι πρακτικά αδύνατο να παρατηρήσουμε τον ίδιο χρόνο δύο φορές (όχι προσεγγιστικά αλλά ακριβώς). Έχει όμως νόημα να μετρήσουμε πόσες φορές (από τις N) ο χρόνος αυτός πέφτει μέσα σε εάν διάστημα, π.χ. ανάμεσα σε 2 και 3 λεπτά. Έχει δηλ. νόημα να μιλήσουμε για την πιθανότητα να συμβεί $2 \leq t \leq 3$.

11.1.6 Ύψος και βάρος

Το πείραμα: Ανοίγουμε τον τηλεφωνικό κατάλογο της πόλης μας και επιλέγουμε ένα τυχαίο άτομο. Το παίρνουμε τηλ. και ρωτάμε το ύψος και το βάρος του.
Το αποτέλεσμα: Δύο πραγματικοί αριθμοί H και W. Υποθέτουμε ότι $0 \leq H \leq 2.5$ (μέτρα) και $0 \leq W \leq 300$ (κιλά).

Εδώ το σύνολο των δυνατών αποτελεσμάτων είναι τα ζεύγη (H, W), όπου τα H και W πληρούν τις άνω ανισότητες. Όπως και στο Παράδειγμα της §11.1.5 το σύνολο των δυνατών αποτελεσμάτων είναι υπαραριθμήσιμο.

11.2 Δειγματικοί χώροι, ενδεχόμενα, η πιθανότητά τους

Δοθέντος ενός πειράματος που θέλουμε να μελετήσουμε πιθανοθεωρητικά η πρώτη δουλειά που πρέπει να γίνει είναι να καταλάβουμε ποια ακριβώς είναι τα δυνατά αποτελέσματα αυτού του πειράματος.

Ορισμός 11.1
(Δειγματικός χώρος) Δειγματικός χώρος Ω *ενός πειράματος ονομάζεται το σύνολο των δυνατών αποτελεσμάτων του.*

Αν σταματήσουμε εδώ τότε φυσικά δεν έχουμε κάνει τίποτα που θα μας βοηθήσει στην πιθανοθεωρητική ανάλυση αφού έχουμε μόνο μιλήσει για τα *δυνατά* αποτελέσματα και όχι για τα *πιθανά*. Γι΄ αυτό το λόγο σε κάθε στοιχείο του δειγματικού χώρου αντιστοιχίζουμε ένα αριθμό p που δηλώνει πόσο πιθανό είναι το στοιχείο αυτό να εμφανιστεί.

Ορισμός 11.2
Έστω $\Omega = \{\omega_1, \omega_2, \ldots\}$ ένας πεπερασμένος ή αριθμήσιμος δειγματικός χώρος ενός πειράματος. Ονομάζουμε κατανομή πιθανότητας στον Ω *μια συνάρτηση $p : \Omega \to [0, 1]$ με την ιδιότητα*

$$\sum_{j=1}^{|\Omega|} p(\omega_j) = 1. \tag{11.2}$$

Εδώ $|\Omega|$ συμβολίζει τον πληθάριθμο του συνόλου $|\Omega|$.

Ο λόγος που που περιοριζόμαστε, προς το παρόν, σε αριθμήσιμους δειγματικούς χώρους, αφήνοντας έξω από τη μελέτη μας πειράματα όπως αυτό της §11.1.5 όπου ο δειγματικός χώρος είναι αυτός των πραγματικών αριθμών (υπεραριθμήσιμος) είναι ότι το αξίωμα (11.2) πρέπει να αντικατασταθεί με κάτι άλλο και η συνάρτηση p δεν είναι πια μια συνάρτηση στα στοιχεία του Ω. Από δώ και στο εξής θα μιλάμε αποκλειστικά για αριθμήσιμους δειγματικούς χώρους εκτός από ορισμένες περιπτώσεις οπότε και θα το ξεκαθαρίζουμε.

Παράδειγμα 11.1
Ο δειγματικός χώρος του τιμίου (έχει δηλ. ίδια πιθανότητα να έρθει κορώνα ή γράμματα) νομίσματος (δες §11.1.1) είναι ο $\Omega = \{K, \Gamma\}$. Η κατανομή πιθανότητας στον Ω είναι η $p(K) = p(\Gamma) = 1/2$.

Παράδειγμα 11.2
Για το τίμιο ζάρι της §11.1.2 έχουμε $\Omega = \{1, 2, 3, 4, 5, 6\}$ και η κατανομή πιθανότητας δίδεται από τη συνάρτηση $p : \Omega \to [0, 1]$ που είναι σταθερή στον Ω, έχουμε δηλ. $p(1) = p(2) = p(3) = p(4) = p(5) = p(6) = 1/6$. Η τιμή 1/6 προκύπτει από την (11.2) και την παραδοχή (τιμιότητα) που κάναμε ότι όλες οι τιμές είναι ισοπίθανες.

Ορισμός 11.3
(Ομοιόμορφη κατανομή) *Μια κατανομή πιθανότητας $p : \Omega \to [0, 1]$ σε ένα δειγματικό χώρο Ω λέγεται* ομοιόμορφη *αν είναι σταθερή στο Ω.*

Με βάση τον προηγούμενο ορισμό μπορούμε να λέμε ότι το τίμιο νόμισμα και το τίμιο ζάρι έχουν και τα δύο την ομοιόμορφη κατανομή, πάνω βέβαια σε διαφορετικούς δειγματικούς χώρους.

Παράδειγμα 11.3
Στο παράδειγμα της §11.1.4 έχουμε $\Omega = \mathbb{N} \cup \{\infty\} = \{1, 2, 3, \ldots, \infty\}$. *Προσέξτε εδώ ότι η τιμή* ∞ *είναι δυνατή τιμή για το πείραμα: είναι θεωρητικά δυνατό ένα ζευγάρι να μην κάνει ποτέ αγόρι οπότε θα αποκτήσει (εις το διηνεκές) άπειρα το πλήθος κορίτσια.*

Η κατανομή πιθανότητας γι'αυτό το παράδειγμα δίνεται από τη συνάρτηση $p : \Omega \to [0, 1]$

$$p(\omega) = \begin{cases} 0 & \alpha\nu\ \omega = \infty \\ 2^{\omega} & \alpha\lambda\lambda\iota\omega\varsigma \end{cases}$$

Θα το αποδείξουμε αυτό αργότερα. Πρός το παρόν το μόνο που είναι εύκολο να δούμε είναι ότι $p(1) = 1/2$ *αφού κάνει η οικογένεια συνολικά μόνο ένα παιδί μόνο αν το πρώτο παιδί είναι αγόρι, και αυτό συμβαίνει με πιθανότητα 1/2.*

Παρ' ότι η τιμή $\omega = \infty$ *είναι δυνατή, εφ' όσον έχει πιθανότητα 0 μπορούμε να την αγνοήσουμε. Με άλλα λόγια, όσον αφορά την πιθανοθεωρητική ανάλυση του πειράματος, στην οποία εν γένει αγνοούμε πράγματα που έχουν πιθανότητα ίση με 0 να συμβούν, μπορούμε να θεωρούμε ότι ο δειγματικός χώρος είναι απλά ο* $\Omega' = \mathbb{N}$.

Ορισμός 11.4
(Ενδεχόμενα) Ενδεχόμενο *ονομάζεται ένα οποιοδήποτε υποσύνολο του δειγματικού χώρου, ένα οποιοδήποτε δηλ. στοιχείο του* $\mathcal{P}(\Omega)$.

Σε σχέση με ένα πείραμα θα λέμε ότι το ενδεχόμενο $A \subseteq \Omega$ *ισχύει αν το αποτέλεσμα του πειράματος ανήκει στο* A.

✏ **11.2**
Αν $|\Omega| = n < \infty$ *δείξτε ότι* $|\mathcal{P}(\Omega)| = 2^n$.

Με τη βοήθεια της κατανομής πιθανότητας $p : \Omega \to [0, 1]$ ορίζουμε τώρα τη *συνολοσυνάρτηση* (δηλ. μια συνάρτηση που ορίζεται πάνω σε σύνολα). της πιθανότητας, που επίσης θα ονομάζουμε κατανομή πιθανότητας, ως εξής.

Ορισμός 11.5
(Συνολοσυνάρτηση πιθανότητας) *Αν* Ω *δειγματικός χώρος με κατανομή πιθανότητας* $p : \Omega \to [0, 1]$ *ορίζουμε τη συνάρτηση* $\mathbb{P} : \mathcal{P}(\Omega) \to [0, 1]$ *με*

$$\mathbf{Pr}[A] = \sum_{a \in A} p(a). \tag{11.3}$$

Με άλλα λόγια η πιθανότητα $\mathbf{Pr}[A]$ *ενός ενδεχομένου* $A \subseteq \Omega$ *προκύπτει αν προσθέσουμε τις τιμές* $p(a)$ *για όλα τα στοιχεία του* A.

Παράδειγμα 11.4
Στο παράδειγμα του ζαριού (§11.1.2) το ενδεχόμενο $A = \{2, 4, 6\}$ *ισχύει μετά την εκτέλεση του πειράματος αν το αποτέλεσμα είναι άρτιο. Έχουμε*

$$\mathbf{Pr}[A] = p(2) + p(4) + p(6) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = 1/2.$$

Παράδειγμα 11.5
Στο παράδειγμα της §11.1.4 το ενδεχόμενο $A = \{1, 2, 3\}$ *ισχύει αν η οικογένεια αποκτήσει τελικά μέχρι και τρία παιδιά. Έχουμε*

$$\mathbf{Pr}[A] = p(1) + p(2) + p(3) = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} = 7/8.$$

✏ **11.3**
Στο πείραμα της §11.1.4 έστω $A = \{2k : \ k = 1, 2, 3, \ldots\}$ *το ενδεχόμενο η οικογένεια να αποκτήσει άρτιο αριθμό παιδιών. Υπολογίστε την* $\mathbf{Pr}[A]$.

Χρησιμοποιήστε την Άσκηση 1.20.

Παρατήρηση 11.1
Έστω A και B δύο ενδεχόμενα. Τότε το να ζητήσουμε να ισχύει το ενδεχόμενο $A \cup B$ είναι σα να ζητάμε να ισχύει ένα τουλάχιστον από τα A και B (μπορεί και τα δύο). Το να ζητήσουμε να ισχύει το ενδεχόμενο $A \cap B$ είναι σα να ζητάμε να ισχύουν και τα δύο ενδεχόμενα A και B.

✏ **11.4**
Στο παράδειγμα της §11.1.4 έστω $A = \{1, \ldots, 10\}$ και $B = \{3k : \ k \in \mathbb{N}\}$ δύο ενδεχόμενα. Περιγράψτε τι σημαίνει το κάθε ένα από αυτά όπως και το τι σημαίνουν τα ενδεχόμενα $A \cap B$ και $A \cup B$.

✏ **11.5**
Στο παράδειγμα της §11.1.3 γράψτε ποια στοιχεία απαρτίζουν το ενδεχόμενο το δεύτερο νόμισμα να δείξει κάτι διαφορετικό από το πρώτο και βρείτε την πιθανότητά του.

✏ **11.6**
Σε ένα κουτί μέσα βρίσκονται τρείς βώλοι, ένας κόκκινος, ένας πράσινος κι ένας μπλέ. Το πείραμά μας συνίσταται στο να τραβήξουμε ένα βώλο, να σημειώσουμε το χρώμα του, να τον επανατοποθετήσουμε μέσα στο κουτί, να τραβήξουμε πάλι ένα βώλο και να σημειώσουμε και αυτού το χρώμα.

Ποιος είναι ο δειγματικός χώρος του πειράματος; Ποια η κατανομή πιθανότητας στα στοιχεία του αν όλοι οι βώλοι που είναι μέσα στο κουτί είναι εξίσου πιθανό να τραβηχτούν κάθε φορά;

Απαντήστε στο ίδιο ερώτημα αν το πείραμα τροποιηθεί ως εξής: αφού τραβήξουμε πρώτο βώλο, δεν τον επανατοποθετούμε στο κουτί, *αλλά απλά τραβάμε και τον δεύτερο από τους δύο εναπομείναντες.*

Ορισμός 11.6
(Επεκτεταμένοι φυσικοί αριθμοί) *Το σύνολο των επεκτεταμένων φυσικών αριθμών είναι το*

$$\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\} = \{1, 2, 3, \ldots, \infty\}.$$

Όταν λοιπόν λέμε $n \in \overline{\mathbb{N}}$ εννοούμε ότι ο αριθμός n είναι είτε ένας φυσικός αριθμός είτε το ∞. Π.χ., αν έχουμε ένα άθροισμα

$$\sum_{n=1}^{N} a_n$$

όπου $N \in \overline{\mathbb{N}}$, εννούμε ότι είτε μιλάμε για πεπερασμένο άθροισμα είτε για άπειρο.

Θεώρημα 11.1
Η συνολοσυνάρτηση πιθανότητας έχει τις εξής ιδιότητες ($m \in \overline{\mathbb{N}}$):

1. $\mathbf{Pr}[\emptyset] = 0$, $\mathbf{Pr}[\Omega] = 1$.
2. $\mathbf{Pr}[A^c] = 1 - \mathbf{Pr}[A]$, *για κάθε ενδεχόμενο A.*
3. *(*Προσθετικότητα*) Αν $A_1, A_2, \ldots, A_m$ είναι ξένα μεταξύ τους ενδεχόμενα τότε*

$$\mathbf{Pr}\left[\bigcup_{j=1}^{m} A_j\right] = \sum_{j=1}^{m} \mathbf{Pr}[A_j]. \tag{11.4}$$

4. *(*Υποπροσθετικότητα*) Αν $A_1, A_2, \ldots, A_m$ είναι ενδεχόμενα, όχι απαραίτητα ξένα ανά δύο, τότε*

$$\mathbf{Pr}\left[\bigcup_{j=1}^{m} A_j\right] \leq \sum_{j=1}^{m} \mathbf{Pr}[A_j]. \tag{11.5}$$

5. *Αν A και B είναι δύο ενδεχόμενα τότε*

$$\mathbf{Pr}[A \cup B] = \mathbf{Pr}[A] + \mathbf{Pr}[B] - \mathbf{Pr}[A \cap B]. \tag{11.6}$$

Απόδειξη

Τα τρία πρώτα είναι άμεσες συνέπειες της (11.3) και της (11.2).

Για το 4 αν χρησιμοποιήσουμε τον ορισμό (11.3) στα δύο μέλη της ανισότητας που έχουμε να αποδείξουμε, παρατηρούμε ότι στο αριστερό μέλος έχουμε ακριβώς τις ποσότητες $p(x)$ για όλα τα $x \in \bigcup_{j=1}^{m} A_j$, μια φορά την κάθε μια, ενώ στο δεξί μέλος έχουμε τις ίδιες ποσότητες $p(x)$ αλλά τόσες φορές την κάθε μια όσα και τα A_j στα οποία ανήκει το x και πάντως τουλάχιστον μια φορά. Η ανισότητα ισχύει προφανώς μια και $p(x) \geq 0$.

Για το 5 επιχειρηματολογούμε όπως και στο προηγούμενο: στο αριστερό μέλος έχουμε το άθροισμα των $p(x)$ για $x \in A \cup B$ ενώ στο δεξί έχουμε στο άθροισμα $\mathbf{Pr}[A] + \mathbf{Pr}[B]$ το άθροισμα των ίδιων $p(x)$ με τη διαφορά ότι για τα $x \in A \cap B$ το $p(x)$ εμφανίζεται δύο φορές. Ο προσθετέος $-\mathbf{Pr}[A \cap B]$ στο δεξί μέλος διορθώνει αυτή τη διαφορά.

■

Παρατήρηση 11.2

Είναι πολύ εύκολο να αποδειχθεί (κάντε το) αλλά και πάρα πολύ σημαντικό σε διάφορες αποδείξεις και εφαρμογές ότι αν $A \subseteq B$ τότε $\mathbf{Pr}[A] \leq \mathbf{Pr}[B]$. Επίσης είναι πολύ σημαντική η απλή συνεπαγωγή

$$\mathbf{Pr}[A] > 0 \Longrightarrow A \neq \emptyset.$$

Αυτή η τελευταία συνεπαγωγή, με την οποία αποδεικνύει κανείς ότι ένα σύνολο δεν είναι κενό αποδεικνύοντας πρώτα ότι η πιθανότητά του δεν είναι 0, αποτελεί το θεμέλιο λίθο της λεγόμενης πιθανοθεωρητικής μεθόδου*, παρόμοιας με την* υπαρξιακή μέθοδο*, στην οποία αποδεικνύει κανείς την ύπαρξη ενός αντικειμένου με πολύ έμμεσο τρόπο, φτιάχνοντας πρώτα ένα πιθανοθεωρητικό μοντέλο γι' αυτό το αντικείμενο που «δουλεύει» με θετική πιθανότητα. Θα έχουμε αργότερα την ευκαιρία να δούμε κάποια παραδείγματα αυτής της μεθόδου.*

✏ **11.7**

Αν A_i, $i = 1, \ldots, m$, $m \in \overline{\mathbb{N}}$, είναι ενδεχόμενα με $\mathbf{Pr}[A_i \cap A_j] = 0$ για κάθε $i \neq j$ δείξτε ότι ισχύει (όπως και όταν $A_i \cap A_j = \emptyset$)

$$\mathbf{Pr}\left[\bigcup_{i=1}^{m} A_i\right] = \sum_{i=1}^{m} \mathbf{Pr}[A_i].$$

✏ **11.8**

Αν A, B, C ενδεχόμενα δείξτε ότι

$$\mathbf{Pr}[A \cup B \cup C] = \mathbf{Pr}[A] + \mathbf{Pr}[B] + \mathbf{Pr}[C]$$

$$- \mathbf{Pr}[A \cap B] - \mathbf{Pr}[B \cap C] - \mathbf{Pr}[C \cap A] + \mathbf{Pr}[A \cap B \cap C].$$

Παράδειγμα 11.6

Έστω A και B δύο ενδεχόμενα, και έστω ότι $\mathbf{Pr}[A] = 3/4$ και $\mathbf{Pr}[B] = 1/3$. Μόνο με αυτή την πληροφορία τι μπορούμε να συμπεράνουμε για την ποσότητα $\mathbf{Pr}[A \cap B]$;

Σίγουρα δε μπορούμε να την υπολογίσουμε ακριβώς. Μπορούμε όμως να έχουμε μια εκτίμηση των ορίων στα οποία κινείται. Συγκεκριμένα μπορούμε να δείξουμε ότι

$$\frac{1}{12} \leq \mathbf{Pr}[A \cap B] \leq \frac{1}{3}.$$

Από το Θεώρημα 11.1 έχουμε

$$\mathbf{Pr}[A \cap B] = \mathbf{Pr}[A] + \mathbf{Pr}[B] - \mathbf{Pr}[A \cup B] \leq \mathbf{Pr}[B] = \frac{1}{3},$$

αφού $\mathbf{Pr}[A \cup B] \geq \mathbf{Pr}[A]$. *Έχουμε δείξει το άνω φράγμα. Για το κάτω φράγμα έχουμε*

$$\mathbf{Pr}[A \cap B] = \mathbf{Pr}[A] + \mathbf{Pr}[B] - \mathbf{Pr}[A \cup B] \geq \frac{3}{4} + \frac{1}{3} - 1 = \frac{1}{12}.$$

Στην τελευταία ανισότητα χρησιμοποιήσαμε απλά ότι $\mathbf{Pr}[A \cup B] \leq 1$.

✏ **11.9**
Έστω ο δειγματικός χώρος $\Omega = \{a, b, c\}$ *με την κατανομή πιθανότητας* $p(a) = 1/3$, $p(b) = 5/12$, $p(c) = 1/4$. *Δείξτε ότι αν πάρουμε τα ενδεχόμενα* $A = \{a, b\}$, $B = \{a\}$ *τότε πιάνεται το άνω όριο στην ανισότητα του Παραδείγματος 11.6.*

Φτιάξτε ομοίως ένα άλλο απλό δειγματικό χώρο με την κατάλληλη κατανομή πιθανότητας που να δείχνει ότι και το κάτω όριο της ανισότητας του Παραδείγματος 11.6 μπορεί να πιάνεται σε κάποια παραδείγματα, και άρα ότι η ανισότητα που δείξαμε στο Παρ. 11.6 είναι η καλύτερη δυνατή που μπορεί κανείς να δείξει με τα δεδομένα που μας δόθηκαν.

Το θεώρημα που ακολουθεί, αν και πολύ απλό στην απόδειξή του, θα μας είναι επανειλλημένως χρήσιμο.

Θεώρημα 11.2
(Νόμοι de Morgan) Αν A_j, $j = 1, 2, \ldots, m$, $m \in \overline{\mathbb{N}}$, *είναι ενδεχόμενα σε ένα χώρο* Ω *τότε έχουμε*

$$\left(\bigcup_{j=1}^{m} A_j\right)^c = \bigcap_{j=1}^{m} A_j^c \tag{11.7}$$

και

$$\left(\bigcap_{j=1}^{m} A_j\right)^c = \bigcup_{j=1}^{m} A_j^c \tag{11.8}$$

Απόδειξη

Ας δείξουμε πρώτα την (11.7). Πρόκειται για μια ισότητα συνόλων. Αρκεί λοιπόν να πάρουμε το τυχόν x που ανήκει στο αριστερό μέλος και να δείξουμε ότι ανήκει και στο δεξί μέλος, και επίσης το τυχόν σημείο που ανήκει στο δεξί και να δείξουμε ότι ανήκει στο αριστερό.

Έστω λοιπόν $x \in \left(\bigcup_{j=1}^{m} A_j\right)^c$. Αυτό σημαίνει ότι $x \notin \bigcup_{j=1}^{m} A_j$ και αυτό με τη σειρά του ότι το x δεν ανήκει σε κανένα A_j. Δηλαδή το x ανήκει σε όλα τα A_j^c, άρα και στην τομή τους, που είναι και το δεξί μέλος. Ομοίως αποδεικνύεται (άσκηση για τον αναγνώστη) ότι αν το x ανήκει στο δεξί μέλος τότε ανήκει και στο αριστερό.

Έχοντας δείξει την (11.7) μπορούμε να τη χρησιμοποιήσουμε για να δείξουμε την (11.8) (ή μπορούμε να επαναλάβουμε για την (11.8) μια απόδειξη όπως αυτή που δώσαμε για την (11.7)). Πράγματι, παρατηρώντας ότι για κάθε σύνολο A έχουμε $(A^c)^c = A$ και χρησιμοποιώντας στη θέση των συνόλων A_j της (11.7) τα σύνολα A_j^c παίρνουμε ακριβώς την (11.8).
■

✏ **11.10**
Έστω A, B, C *ενδεχόμενα. Βρείτε εκφράσεις, χρησιμοποιώντας τα* A, B, C *και συνολοθεωρητικές πράξεις, για τα ενδεχόμενα:*

1. *Συμβαίνει μόνο το* A.
2. *Συμβαίνει το* A *και το* B *αλλά όχι το* C.
3. *Συμβαίνει τουλάχιστον ένα από τα* A, B, C.
4. *Συμβαίνουν όλα τα* A, B, C.

5. *Συμβαίνει το πολύ ένα από τα A, B, C.*

✏ **11.11**
Δώστε μια συνολοθεωρητική συνθήκη για την πρόταση «Αν συμβαίνει το ενδεχόμενο A τότε συμβαίνει το B ή το C».

Επίσης για την πρόταση «δε γίνεται να συμβαίνουν ταυτόχρονα τα A και B».

✏ **11.12**
Ρίχνουμε ζεύγος τιμίων ζαριών. Ποια τα στοιχεία του ενδεχομένου «τα δυο αποτελέσματα έχουν άθροισμα 4»; Ποια η πιθανότητα του ενδεχομένου αυτού;

✏ **11.13**
Οι παίκτες Α και Β παίζουν το εξής παιχνίδι. Ο Α έχει μπροστά του τρία κουτιά, το περιεχόμενο των οποίων βλέπει. Τα δύο κουτιά είναι άδεια και το ένα έχει μέσα ένα νόμισμα. Σκοπός του παίκτη Β είναι να πάρει το νόμισμα.

Οι κανόνες του παιχνιδιού είναι οι εξής: (α) ο Β διαλέγει ένα κουτί και το δείχνει στον Α, (β) ο Α υποχρεούται να επιλέξει ένα άδειο κουτί που δεν είναι αυτό που έδειξε ο Β και να το υποδείξει στον Β, και (γ) ο Β έχει τώρα την ευκαιρία να επιμείνει στην αρχική του επιλογή ή να επιλέξει το άλλο κλειστό κουτί.

Ο Β μπορεί να παίξει με τις εξής τρεις στρατηγικές:

1. *Ο Β πάντα εμμένει στην αρχική του επιλογή.*
2. *Ο Β στρίβει ένα νόμισμα και ξαναεπιλέγει τυχαία ανάμεσα στα δύο εναπομείναντα κλειστά κουτιά.*
3. *Ο Β πάντα αλλάζει κουτί.*

Ποια είναι η πιθανότητα να βρεί ο Β το νόμισμα αν ακολουθήσει κάθε μια από αυτές τις στρατηγικές;

11.2.1 Υπεραριθμήσιμοι δειγματικοί χώροι

Το πείραμα: Έχουμε ένα στρογγυλό στόχο ακτίνας R και πετάμε σε αυτό ένα βέλος.
Το αποτέλεσμα: Το σημείο (x, y) στο οποίο έπεσε το βέλος.

Και πάλι παρατηρούμε, όπως και στο παράδειγμα της §11.1.5 ότι το σύνολο Ω των δυνατών αποτελεσμάτων, που στην προκειμένη περίπτωση είναι τα σημεία του στόχου, είναι υπεραριθμήσιμο.

Η υπόθεσή μας εδώ είναι ότι δύο ενδεχόμενα A και B, υποσύνολα δηλ. του δίσκου, με το ίδιο εμβαδό έχουν την ίδια πιθανότητα να χτυπηθούν. Από την προσθετικότητα που πρέπει να πληροί η συνολοσυνάρτηση της πιθανότητας προκύπτει λοιπόν ότι για κάθε $A \subseteq \Omega$

$$\mathbf{Pr}[A] = (\text{εμβαδό του } A) \,/\, \pi R^2.$$

Ποια θα μπορούσε να είναι τότε η κατανομή πιθανότητας $p : \Omega \to [0, 1]$ που παράγει την άνω συνολοσυνάρτηση; Η μόνη αποδεκτή λύση συμβατή με την άνω ισότητα θα έπρεπε να είναι η $p(x) \equiv 0$, η οποία φυσικά είναι άχρηστη. Το συμπέρασμα είναι ότι δε μπορεί φυσικά να οριστεί τέτοια συνάρτηση p.

Η λύση σε αυτό το πρόβλημα είναι η εξής. Σε δειγματικούς χώρους που είναι υπεραριθμήσιμοι δε χρησιμοποιούμε μια συνάρτηση $p : \Omega \to [0, 1]$ για να ορίσουμε τη συνολοσυνάρτηση $\mathbf{Pr}[\cdot]$ αλλά ορίζουμε τη συνολοσυνάρτηση αυτή κατ' ευθείαν ως μια συνολοσυνάρτηση που πληροί τα παρακάτω (για να είμαστε ακριβέστεροι θα πρέπει να πούμε ότι συνήθως δεν είναι όλα τα υποσύνολα του δειγματικού χώρου ενδεχόμενα):

Αξιώματα της συνολοσυνάρτησης πιθανότητας

1. $0 \leq \mathbf{Pr}[A] \leq 1$ για κάθε A.
2. $\mathbf{Pr}[\Omega] = 1$
3. Αν $A_1, A_2, \ldots$ είναι ανά δύο ξένα τότε $\mathbf{Pr}\left[\bigcup_j A_j\right] = \sum_j \mathbf{Pr}[A_j]$.

11.2.2 Ενδεχόμενα με πιθανότητα 0

Ορισμός 11.7
Ένα ενδεχόμενο $A \subseteq \Omega$ λέγεται σχεδόν σίγουρο *αν* $\mathbf{Pr}[A^c] = 0$. *Λέγεται* σχεδόν αδύνατο *αν* $\mathbf{Pr}[A] = 0$. *Λέμε ότι κάτι (ένα ενδεχόμενο δηλ.) συμβαίνει σχεδόν σίγουρα αν συμβαίνει με πιθανότητα 1.*

Παράδειγμα 11.7
Στο παράδειγμα της §11.1.4 είναι σχεδόν σίγουρο ότι η οικογένεια θα αποκτήσει πεπερασμένο αριθμό από παιδιά, αφού το συμπληρωματικό ενδεχόμενο, ο αριθμός των παιδιών να είναι ∞, έχει πιθανότητα 0.

Παρατήρηση 11.3
Εύκολα βλέπουμε (υποπροσθετικότητα) ότι αν A_i, $i = 1, 2, \ldots, m$, είναι σχεδόν αδύνατα τότε και η ένωσή τους επίσης είναι σχεδόν αδύνατη. Είναι σημαντικό εδώ ότι μιλάμε για μια ένωση από αριθμήσιμα σε πλήθος ενδεχόμενα. Είναι λάθος ότι οποιαδήποτε ένωση ενδεχομένων με πιθανότητα 0 έχει πιθανότητα 0. Αυτό θα φανεί καλύτερα αργότερα όταν θα δούμε μη διακριτούς (υπεραριθμήσιμους) δειγματικούς χώρους.

✏ **11.14**
Έστω ακολουθία ενδεχομένων E_k, $k \geq 1$, με $\mathbf{Pr}[E_k] \to 0$. Δείξτε ότι το ενδεχόμενο $E = \bigcap_{k\geq 1} E_k$ είναι σχεδόν αδύνατο.

✏ **11.15**
Έστω σχεδόν σίγουρα ενδεχόμενα E_k, $k \geq 1$. Δείξτε ότι σχεδόν σίγουρα ισχύουν όλα τα E_k.

✏ **11.16**
Έστω ενδεχόμενα A_k, $k \geq 1$. Ορίζουμε τα ενδεχόμενα

$$\limsup_k A_k = \bigcap_{k\geq 1} \bigcup_{n\geq k} A_n \text{ και } \liminf_k A_k = \bigcup_{k\geq 1} \bigcap_{n\geq k} A_n. \tag{11.9}$$

Δείξτε ότι το ενδεχόμενο $\limsup_k A_k$ ισχύει ακριβώς όταν ισχύουν άπειρα από τα A_k και το ενδεχόμενο $\liminf_k A_k$ ακριβώς όταν ισχύουν τελικά *όλα τα A_k, όταν δηλ. υπάρχει κάποιο k_0 ώστε να ισχύουν όλα τα A_k, $k \geq k_0$.*

✏ **11.17**
Αν έχουμε ενδεχόμενα A_k, $k \geq 1$, με $\sum_{k=1}^{\infty} \mathbf{Pr}[A_k] < \infty$ τότε είναι σχεδόν αδύνατο να ισχύουν άπειρα από τα A_k.

11.3 Υπό συνθήκη πιθανότητα

Το πείραμα: Σ' ένα κουτί μέσα βρίσκονται δέκα βώλοι με ονόματα 1 έως 10. Τραβάμε ένα βώλο στην τύχη.
Το αποτέλεσμα: Υποθέτουμε ότι κάποιος μας εγγυάται ότι $X \geq 5$. (Για παράδειγμα, αυτός που εκτελεί το πείραμα ελέγχει αν η συνθήκη $X \geq 5$ ισχύει και, αν όχι, ακυρώνει το πείραμα και το εκτελεί ξανά. Αντίθετα αν η συνθήκη $X \geq 5$ ισχύει τότε μας αναφέρει ότι αυτό συμβαίνει.) Ποιος βώλος X τραβήχτηκε.

Αν δε βάζαμε τη συνθήκη $X \geq 5$ θα είχαμε το δειγματικό χώρο $\Omega = \{1, \ldots, 10\}$ και τη συνάρτηση πιθανότητας $p(x) = 0.1$ για $x \in \Omega$. Εφόσον όμως είναι εγγυημένο ότι $X \geq 5$ τα δυνατά αποτελέσματα είναι πλέον τα 5 έως 10, και εφ' όσον εξακολουθούν να είναι ισοπίθανα έχουν όλα τώρα πιθανότητα 1/6.

Ορισμός 11.8
(Υπό συνθήκη πιθανότητα ή δεσμευμένη πιθανότητα) *Έστω δειγματικός χώρος Ω και ενδεχόμενα A, B, με $\mathbf{Pr}[B] > 0$. Ορίζουμε την* υπό συνθήκη πιθανότητα *του A δεδομένου του B ως την ποσότητα*

$$\mathbf{Pr}[A \mid B] = \frac{\mathbf{Pr}[A \cap B]}{\mathbf{Pr}[B]}. \tag{11.10}$$

Η ποσότητα αυτή δεν ορίζεται αν $\mathbf{Pr}[B] = 0$.

Παράδειγμα 11.8
Στο προηγούμενο πείραμα, αν $A = \{X \leq 5\}$ και $B = \{Χαρτιο\}$ ποια η υπό συνθήκη πιθανότητα $\mathbf{Pr}[A \mid B]$;

Εφαρμόζοντας τον ορισμό (11.10) και παρατηρώντας ότι $A \cap B = \{2, 4\}$ παίρνουμε $\mathbf{Pr}[A \mid B] = \frac{2/10}{5/10} = \frac{2}{5}$. Έχουμε υπολογίσει την πιθανότητα να βγάλουμε ένα βώλο με αριθμό το πολύ 5 αν γνωρίζουμε ότι αυτό που τραβήξαμε είναι άρτιο.

✏ **11.18**
Για τυχόν ενδεχόμενο A σε ένα δειγματικό χώρο Ω υπολογίστε τα $\mathbf{Pr}[A \mid A]$, $\mathbf{Pr}[A \mid A^c]$, $\mathbf{Pr}[A \mid \Omega]$.

Παράδειγμα 11.9
Έχουμε τρία κουτιά με δύο θήκες το καθένα. Κάθε θήκη έχει μέσα ένα βώλο. Στο πρώτο κουτί κι οι δύο βώλοι είναι μαύροι, στο δεύτερο κι οι δύο άσπροι και στο τρίτο κουτί ένας άσπρος κι ένας μαύρος. Επιλέγουμε στην τύχη ένα κουτί και μια από τις δύο θήκες του. Ανοίγουμε τη θήκη και βλέπουμε ένα μαύρο βώλο. Ποια η πιθανότητα στην άλλη θήκη του ίδιου κουτιού ο βώλος να είναι επίσης μαύρος;

Ας γράψουμε A_1 για το ενδεχόμενο να έχουμε επιλέξει το πρώτο κουτί, A_2 για το δεύτερο και A_3 για το τρίτο. Επίσης ας είναι B το ενδεχόμενο ότι στη θήκη που ανοίγουμε έχει μαύρο βώλο. Για να έχει και η δεύτερη θήκη του ίδιου κουτιού μαύρο βώλο πρέπει αναγκαστικά το κουτί να είναι το πρώτο. Πρέπει δηλ. να υπολογίσουμε την ποσότητα

$$\mathbf{Pr}[A_1 \mid B] = \frac{\mathbf{Pr}[A_1 \cap B]}{\mathbf{Pr}[B]}.$$

Όμως $A_1 \subseteq B$, δηλ. αν ισχύει το A_1 σίγουρα ισχύει και το B, οπότε $A_! \cap B = A_1$ και $\mathbf{Pr}[A_i] = 1/3$ αφού επιλέγεται το κάθε κουτί με ίση πιθανότητα. Επίσης $\mathbf{Pr}[B] = 1/2$ αφού υπάρχουν συνολικά τόσοι μαύροι βώλοι όσοι και άσπροι κι όλοι οι βώλοι επιλέγονται με την ίδια πιθανότητα. Άρα $\mathbf{Pr}[A_1 \mid B] = \frac{1/3}{1/2} = \frac{2}{3}$.

Θεώρημα 11.3
(Τύπος ολικής πιθανότητας) Έστω B_i, $i = 1, \ldots, m$, $m \in \overline{\mathbb{N}}$, ξένα ανά δύο ενδεχόμενα με

$$\Omega = \bigcup_{i=1}^{m} B_i$$

και $\mathbf{Pr}[B_i] > 0$ για κάθε i. Τότε για κάθε ενδεχόμενο $A \subseteq \Omega$ ισχύει

$$\mathbf{Pr}[A] = \sum_{i=1}^{m} \mathbf{Pr}[A \mid B_i]\mathbf{Pr}[B_i]. \tag{11.11}$$

Ειδικότερα αν $0 < \mathbf{Pr}[B] < 1$ έχουμε για κάθε ενδεχόμενο A

$$\mathbf{Pr}[A] = \mathbf{Pr}[A \mid B]\mathbf{Pr}[B] + \mathbf{Pr}[A \mid B^c](1 - \mathbf{Pr}[B]). \tag{11.12}$$

Απόδειξη

Το δεξί μέλος της (11.11) γράφεται, χρησιμοποιώντας τον Ορισμό 11.8 ως

$$\sum_{i=1}^{m} \mathbf{Pr}[A \cap B_i] = \mathbf{Pr}\left[A \cap \bigcup_{i=1}^{m} B_i\right] = \mathbf{Pr}[A \cap \Omega] = \mathbf{Pr}[A].$$

Στην πρώτη ισότητα χρησιμοποιήσαμε την προσθετικότητα (11.4) της συνολοσυνάρτησης $\mathbf{Pr}[\cdot]$ και το γεγονός ότι τα $A \cap B_i$ είναι ανά δύο ξένα, όπως και την επιμεριστική ιδιότητα της τομής με την ένωση

$$E \cap (F \cup G) = (E \cap F) \cup (E \cap G).$$

Για την (11.12) πάρτε $m = 2$, $B_1 = B$, $B_2 = B^c$.
■

Ορισμός 11.9
(Διαμέριση) *Όταν έχουμε κάποια σύνολα των οποίων η ένωση είναι το* Ω *και είναι ανά δύο ξένα τότε λέμε ότι αυτά αποτελούν μια* διαμέριση *του* Ω*.*

✏ **11.19**
Δείξτε ότι ο τύπος (11.11) *ισχύει για όλες τις διαμερίσεις του* Ω*, ακόμα και αυτές όπου κάποια* B_i *έχουν πιθανότητα 0, αρκεί να παραλειφθούν αυτά τα* B_i *από το δεξί μέλος της* (11.11)*.*

Με άλλα λόγια, αν και η ποσότητα $\mathbf{Pr}[A \mid B]$ *δεν έχει πάντα νόημα, η ποσότητα* $\mathbf{Pr}[A \mid B]\mathbf{Pr}[B] = \mathbf{Pr}[A \cap B]$ *έχει.*

Παρατήρηση 11.4
Το να λέμε ότι τα σύνολα B_i *αποτελούν διαμέριση του δειγματικού χώρου* Ω *είναι ισοδύναμο με το να λέμε ότι σε κάθε έκβαση του πειράματος ισχύει* ακριβώς ένα *από τα* B_i*.*

Παρατήρηση 11.5
Έστω ξένα ανά δύο ενδεχόμενα B_i*,* $i = 1, \ldots, m$*, με* $\bigcup_{i=1}^{m} B_i = \Omega \setminus E$*, όπου* $\mathbf{Pr}[E] = 0$*. Ενώ δηλ. τα* B_i *δεν αποτελούν κατ' ανάγκη διαμέριση του* Ω*, παρ' όλ' αυτά αποτελούν* σχεδόν *μια τέτοια, αφού αυτό που τους λείπει για να είναι κανονική διαμέριση είναι ένα σύνολο, το* E*, που έχει πιθανότητα 0.*

*Δηλ. με πιθανότητα 1 (*σχεδόν σίγουρα *όπως λέμε στη Θεωρία Πιθανοτήτων) όποτε γίνει το πείραμα θα ισχύει ακριβώς ένα από τα* B_i*.*

✏ **11.20**
Στην Παρατήρηση 11.5 είδαμε πώς μπορούμε να χαλαρώσουμε τις συνθήκες ορισμού μιας διαμέρισης B_i *του* Ω *ώστε να ισχύει σχεδόν σίγουρα ακριβώς ένα από τα* B_i*. Μπορούν όμως να χαλαρώσουν περαιτέρω οι συνθήκες αυτές ώστε να έχουμε το ίδιο αποτέλεσμα.*

Βρείτε πώς πρέπει να χαλαρώσουμε τη συνθήκη ότι τα B_i *είναι ανά δύο ξένα ώστε να εξακολουθεί να ισχύει σχεδόν σίγουρα ακριβώς ένα από τα* B_i *σε κάθε έκβαση του πειράματος.*

Παράδειγμα 11.10
Σ' ένα κουτί βρίσκονται κόκκινοι, πράσινοι και μπλέ βώλοι σε ποσοστά 30%, 50% και 20% αντίστοιχα. Οι μισοί κόκκινοι βώλοι είναι κούφιοι και το ίδιο ισχύει για τα 2/3 των πράσινων και μπλέ βώλων. Αν διαλέξουμε τυχαία ένα βώλο από το κουτί, ποια η πιθανότητα να είναι κούφιος;

Ορίζουμε A_r, A_g, A_b *να είναι τα ενδεχόμενα επιλογής κόκκινου, πράσινου ή μπλέ βώλου. Αυτά είναι ανά δύο ξένα με πιθανότητες που μας δίδονται:*

$$\mathbf{Pr}[A_r] = 0.3,\ \mathbf{Pr}[A_g] = 0.5,\ \mathbf{Pr}[A_b] = 0.2.$$

οπότε αποτελούν διαμέριση του χώρου και μπορούμε να εφαρμόσουμε τον τύπο ολικής πιθανότητας για το ενδεχόμενο H *του να είναι κούφιος ο βώλος που διαλέξαμε*

$$\begin{aligned}
\mathbf{Pr}[H] &= \mathbf{Pr}[H \mid A_r]\mathbf{Pr}[A_r] + \mathbf{Pr}[H \mid A_g]\mathbf{Pr}[A_g] + \mathbf{Pr}[H \mid A_b]\mathbf{Pr}[A_b] \\
&= \frac{1}{2}0.3 + \frac{2}{3}0.5 + \frac{2}{3}0.2 \\
&= 0.616
\end{aligned}$$

✏ **11.21**
Μια οικογένεια έχει δύο παιδιά. Ποια η πιθανότητα ότι είναι και τα δύο αγόρια δεδομένου ότι τουλάχιστον ένα από αυτά είναι αγόρι; Περιγράψτε το δειγματικό χώρο του πειράματος και υποθέστε ότι όλα τα στοιχεία του είναι ισοπίθανα για να απαντήσετε την ερώτηση.

11.4 Ανεξαρτησία ενδεχομένων

Ορισμός 11.10
(Ανεξαρτησία ενδεχομένων) *Δύο ενδεχόμενα A και B ονομάζονται* ανεξάρτητα *αν* $\mathbf{Pr}[A \cap B] = \mathbf{Pr}[A] \cdot \mathbf{Pr}[B]$.

Γενικότερα αν A_j, $j \in J$, είναι ένα σύνολο ενδεχομένων (το σύνολο J μπορεί να είναι και υπεραριθμήσιμο) αυτό θα λέγεται ανεξάρτητο σύνολο ενδεχομένων *αν για κάθε πεπερασμένο πλήθος από αυτά, έστω $A_{j_1}, \ldots, A_{j_N}$, η πιθανότητα της τομής τους ισούται με το γινόμενο των πιθανοτήτων τους:*

$$\mathbf{Pr}[A_{j_1} \cap \cdots \cap A_{j_N}] = \mathbf{Pr}[A_{j_1}] \cdots \mathbf{Pr}[A_{j_N}].$$

Παρατήρηση 11.6
Ένας πιο φυσιολογικός ορισμός για την ανεξαρτησία δύο ενδεχομένων A και B είναι να απαιτήσουμε να ισχύει

$$\mathbf{Pr}[A \mid B] = \mathbf{Pr}[A].$$

Αυτή η σχέση προκύπτει από τον παραπάνω ορισμό της ανεξαρτησίας διαιρώντας με $\mathbf{Pr}[B]$, αν αυτό φυσικά δεν είναι 0. Μας λέει λοιπόν αυτή η ισότητα ότι αν υποθέσουμε ότι ισχύει το B δεν αλλάζει τίποτα στην πιθανότητα του A να ισχύει. Δεν επηρεάζει δηλ. το ένα γεγονός το άλλο.

Ο ορισμός αυτός, αν και διαισθητικά ελκυστικότερος, έχει το μειονέκτημα ότι (α) δεν μπορούμε να τον επικαλεστούμε εκτός αν $\mathbf{Pr}[B] > 0$, (β) τα A και B δεν εμφανίζονται με συμμετρικό τρόπο σε αυτόν και (γ) δε γενικεύεται εύκολα σε περισσότερα από δύο ενδεχόμενα.

✏ **11.22**
Αν A και B είναι ανεξάρτητα ενδεχόμενα τότε και τα A^c, B είναι και ομοίως και τα A^c, B^c.

✏ **11.23**
Δείξτε ότι αν A και B είναι δύο ξένα ενδεχόμενα με $\mathbf{Pr}[A] > 0$, $\mathbf{Pr}[B] > 0$ τότε αυτά δεν είναι ανεξάρτητα. Ομοίως αν $A \subseteq B$ και $B \neq \Omega$.

Παράδειγμα 11.11
Το πείραμά μας αποτελείται από τη ρίψη ενός τιμίου νομίσματος δύο φορές. Ο δειγματικός χώρος είναι ο

$$\Omega = \{(x, y) : x, y \in \{K, \Gamma\}\}.$$

Ο Ω δηλ. αποτελείται από όλα τα δυνατά ζεύγη αποτελεσμάτων, και έχει συνεπώς 4 στοιχεία. Υποθέτουμε ότι όλα αυτά είναι ισοπίθανα με πιθανότητα 1/4 το καθένα. Αν ορίσουμε $A = \{$το πρώτο νόμισμα είναι $K\}$ και $B = \{$ το δεύτερο νόμισμα είναι $\Gamma\}$ τότε τα A και B είναι ανεξάρτητα αφού $A \cap B = \{(K, \Gamma)\}$ και άρα $\mathbf{Pr}[A \cap B] = 1/4$ ενώ $\mathbf{Pr}[A] = \mathbf{Pr}[B] = 1/2$ αφού καθένα από τα A, B έχει δύο στοιχεία.

Η ανεξαρτησία αυτών των δύο ενδεχομένων αντικατοπτρίζει το γεγονός ότι οι δύο διαφορετικές ρίψεις του νομίσματος δεν επηρεάζουν η μια την άλλη, είναι όπως λέμε ανεξάρτητες ρίψεις.

Παράδειγμα 11.12
Ας υποθέσουμε ότι τα ενδεχόμενα A, B, C, D είναι ανεξάρτητα. Ορίζουμε $E = A \cup B$ και $H = C \cap D$. Τα ενδεχόμενα H και D εξαρτώνται το καθένα από κάποια από τα A, B, C, D αλλά δεν υπάρχει κανένα από τα A, B, C, D από το οποίο να εξαρτώνται τα E και H. Περιμένουμε λοιπόν τα E και H να είναι ανεξάρτητα.

Πράγματι

$$\begin{aligned}
\mathbf{Pr}[E \cap H] &= \mathbf{Pr}[(A \cup B) \cap (C \cap D)] \\
&= \mathbf{Pr}[(A \cap C \cap D) \cup (B \cap C \cap D)] \\
&= \mathbf{Pr}[A \cap C \cap D] + \mathbf{Pr}[B \cap C \cap D] - \mathbf{Pr}[A \cap B \cap C \cap D].
\end{aligned}$$

ενώ

$$\begin{aligned}\mathbf{Pr}[E]\cdot\mathbf{Pr}[H] &= \mathbf{Pr}[A\cup B]\mathbf{Pr}[C\cap D]\\ &= (\mathbf{Pr}[A]+\mathbf{Pr}[B]-\mathbf{Pr}[A\cap B])\mathbf{Pr}[C]\mathbf{Pr}[D]\\ &= \mathbf{Pr}[A\cap C\cap D]+\mathbf{Pr}[B\cap C\cap D]-\mathbf{Pr}[A\cap B\cap C\cap D],\end{aligned}$$

άρα οι δύο ποσότητες είναι ίδιες. Στα παραπάνω χρησιμοποιήσαμε και την ισότητα (11.6).

Παρατήρηση 11.7
Πώς γενικεύεται το Παράδειγμα 11.12; Αν έχουμε κάποια ενδεχόμενα A_i και κάποια B_j, όλα ανεξάρτητα μεταξύ τους, και ενδεχόμενα A και B που ορίζονται μέσω των A_i και B_j αντιστοιχα, για παράδειγμα μέσω συνολοθεωρητικών πράξεων όπως στο Παράδειγμα 11.12, τότε τα A και B είναι ανεξάρτητα. Αν και η απόδειξη δεν είναι ιδιαίτερα δύσκολη δε θα την παρουσιάσουμε εδώ. Θα χρησιμοποιηθεί όμως κατά κόρον.

Παράδειγμα 11.13
Ρίχνουμε τρεις φορές ένα νόμισμα. Υποθέτουμε ότι οι ρίψεις είναι ανεξάρτητες. Τι σημαίνει όμως αυτό ακριβώς;

Ένας τρόπος να εκφραστούμε με ακρίβεια είναι ο εξής. Ονομάζουμε A_i το ενδεχόμενο να έχουμε κορώνα (Κ) στην i-οστή ρίψη, $i=1,2,3$. Η υπόθεση ότι οι ρίψεις είναι ανεξάρτητες σημαίνει ότι τα ενδεχόμενα A_1, A_2, A_3 είναι ανεξάρτητα.

Τι συνέπειες έχει αυτό; Για παράδειγμα εν θέλουμε να υπολογίσουμε την πιθανότητα του να έχουμε ΚΚΓ στις τρεις ρίψεις του νομίσματος αυτή είναι η πιθανότητα του ενδεχομένου $A_1\cap A_2\cap A_3^c$ και, λόγω της ανεξαρτησίας, έχουμε

$$\mathbf{Pr}[A_1\cap A_2\cap A_3^c]=\mathbf{Pr}[A_1]\mathbf{Pr}[A_2]\mathbf{Pr}[A_3^c],$$

και, αν το νόμισμα είναι και τίμιο (ίση πιθανότητα να φέρουμε Κ ή Γ σε μία οποιαδήποτε ρίψη) τότε η πιθανότητα αυτή ισούται με $(\frac{1}{2})^3=\frac{1}{8}$.

Παράδειγμα 11.14
Σε αντιστοιχία με το Παράδειγμα 11.13 τι σημαίνει ότι ρίχνουμε ένα ζάρι τρεις ανεξάρτητες φορές;

Εδώ τα πράγματα περιπλέκονται λίγο σε σχέση με το Παράδειγμα 11.13 μια και σε εκείνο το Παράδειγμα αρκούσε να ξέρουμε το αν φέραμε κορώνα ή όχι για να ξέρουμε το αποτέλεσμα της ρίψης, πράγμα που δεν ισχύει εδώ μια και το πλήθος των δυνατών αποτελεσμάτων μιας ρίψης είναι 6 κι όχι 2.

Ένας τρόπος να θεμελιώσουμε με ακρίβεια την ανεξαρτησία των τριών ρίψεων είναι να ορίσουμε το ενδεχόμενο A_i^j, $i=1,2,3$, $j=1,\ldots,6$, να σημαίνει ότι στην i-οστή ρίψη έχουμε αποτέλεσμα j, και να πούμε ότι για κάθε επιλογή των άνω δεικτών $j_1,\ldots,j_3\in\{1,\ldots,6\}$ τα ενδεχόμενα $A_1^{j_1}, A_2^{j_2}, A_3^{j_3}$ είναι ανεξάρτητα.

Με αυτό τον τρόπο μπορούμε π.χ. να υπολογίσουμε την πιθανότητα να φέρουμε αποτελέσματα 1,2,3 ως την πιθανότητα του ενδεχομένου $A_1^1\cap A_2^2\cap A_3^3$, που, λόγω της ανεξαρτησίας των τριών, ισούται με $1/6^3$.

Πάντως ο πιο απλός τρόπος να θεμελιώσουμε σωστά την έννοια των ανεξάρτητων αυτών ρίψεων θα μας είναι προσιτός αφού μιλήσουμε για τις τυχαίες μεταβλητές.

Η σύμβαση που θα ακολουθούμε από δω και πέρα στην περιγραφή πειραμάτων κωδικοποιείται στον παρακάτω ορισμό.

Ορισμός 11.11
Θα λέμε ότι τα πειράματα $\Pi_1,\ldots,\Pi_m$, $m\in\overline{\mathbb{N}}$, εκτελούνται ανεξάρτητα αν για κάθε επιλογή ενδεχομένων $A_1,\ldots,A_m$ τέτοια ώστε το ενδεχόμενο A_i εξαρτάται μόνο από το πείραμα Π_i, η οικογένεια ενδεχομένων $A_1,\ldots,A_m$ είναι ανεξάρτητη. (Το ότι το ενδεχόμενο A_i εξαρτάται μόνο από το πείραμα Π_i σημαίνει απλά ότι αν γνωρίζουμε το αποτέλεσμα του Π_i και μόνο μπορούμε να αποφασίσουμε αν ισχύει το A_i ή όχι.)

Παρατήρηση 11.8
Το ότι μπορούμε, δεδομένων κάποιων πειραμάτων, να θεωρήσουμε ότι μπορούν να εκτελεστούν ανεξάρτητα θέλει κάποια τεκμηρίωση. Το να πούμε δηλ. την πρόταση

> *Έστω n ανεξάρτητες ρίψεις ενός νομίσματος.*

συνεπάγεται ότι στον προφανή δειγματικό χώρο αυτού του σύνθετου πειράματος

$$\Omega = \{(x_1, \ldots, x_n) : \ x_i \in \{K, \Gamma\}\}$$

μπορούμε να ορίσουμε μια συνάρτηση πιθανότητας $p : \Omega \to [0, 1]$ τέτοια ώστε η απαίτηση του Ορισμού 11.11 να ισχύει. Αυτό δεν είναι δύσκολο αν το πλήθος των ανεξάρτητα εκτελούμενων πειραμάτων είναι πεπερασμένο αλλά είναι αρκετά πιο τεχνικό για $n = \infty$. Στην περίπτωση μάλιστα αυτή ο δειγματικός χώρος δεν είναι καν αριθμήσιμος, οπότε δεν μπορούμε καν να μιλήσουμε για την κατανομή πιθανότητας $p : \Omega \to [0, 1]$ αλλά πρέπει (δείτε §11.2.1) να ορίσει κανείς τη συνολοσυνάρτηση $\mathbf{Pr}[\cdot]$ που πληροί τα αξιώματα της §11.2.1. Θα το θεωρούμε αυτό γνωστό από δω και πέρα.

✏ **11.24**
Δείξτε ότι αν υποθέσουμε ότι έχουμε τρείς ανεξάρτητες ρίψεις ζαριών με βάση τον Ορισμό 11.11 τότε ισχύει η υπόθεση που κάναμε στο Παράδειγμα 11.14.

✏ **11.25**
Ρίχνουμε ένα νόμισμα n φορές. Δείξτε ότι η πιθανότητα να φέρουμε n κορώνες είναι 2^{-n}.

✏ **11.26**
Ρίχνουμε ένα νόμισμα τρεις φορές, και έστω A_{ij} το ενδεχόμενο η i-οστή και η j-οστή ρίψη να φέρουν το ίδιο αποτέλεσμα, $i < j$, $i, j = 1, 2, 3$.

Δείξτε ότι τα τρία αυτά ενδεχόμενα είναι ανά δύο ανεξάρτητα αλλά όχι και τα τρία μαζί.

✏ **11.27**
Σε ένα πληθυσμό από N ζευγάρια όπου το καθένα κάνει ακριβώς δύο παιδιά, τι ποσοστό των ζευγαριών περιμένετε να έχει δύο κόρες;

✏ **11.28**
Ρίχνουμε τυχαία βελάκια σ' ένα στρογγυλό στόχο ακτίνας R. Υποθέτουμε ότι τα βελάκια ακολουθούν την ομοιόμορφη κατανομή, ότι δηλ. αν A και B είναι δύο ισεμβαδικά χωρία μέσα στο στόχο τότε η πιθανότητα να πέσει το βελάκι μέσα στο A και στο B είναι η ίδια. Με άλλα λόγια ακολουθούμε το μοντέλο της §11.2.1. Δείξτε ότι το να πέσει το βελάκι στο αριστερό μισό του δίσκου και το να πέσει στον κάτω μισό δίσκο είναι ανεξάρτητα γεγονότα.

Παράδειγμα 11.15
Επανερχόμαστε στο παράδειγμα της §11.1.4 για να υπολογίσουμε την πιθανότητα η οικογένεια να κάνει k παιδιά, $k \geq 1$. Η ακριβής υπόθεση που κάνουμε εδώ είναι ότι οι διαδοχικές γέννες της οικογένειας είναι ανεξάρτητα πειράματα, και το καθένα από αυτά φέρνει αγόρι ή κορίτσι με ίση πιθανότητα. Ας συμβολίσουμε λοιπόν με A_k το ενδεχόμενο η οικογένεια να αποκτήσει συνολικά k παιδιά, $k \in \overline{\mathbb{N}}$. Ας συμβολίσουμε επίσης με B_i και G_i τα ενδεχόμενα στην i-οστή γέννα το ζευγάρι να αποκτήσει αγόρι ή κορίτσι, αντίστοιχα, $i \in \mathbb{N}$. (Αν και το ζευγάρι σταματά να κάνει παιδιά όταν αποκτήσει αγόρι εμείς ωστόσο μπορούμε ιδεατά να συνεχίσουμε το πείραμα, κι έτσι τα ενδεχόμενα B_i και G_i έχουν νόημα για κάθε $i \in \mathbb{N}$. Με άλλα λόγια θα μπορούσε το πείραμα να έχει διατυπωθεί ως εξής: έχουμε ένα ζευγάρι που κάνει συνέχεια παιδιά, επ' άπειρον, και μας ενδιαφέρει το πότε κάνει το πρώτο αγόρι.)

Προφανώς τότε ισχύει για κάθε $k \in \mathbb{N}$

$$A_k = G_1 \cap G_2 \cap \cdots \cap G_{k-1} \cap B_k.$$

Για να αποκτήσει δηλ. το ζευγάρι k παιδιά συνολικά πρέπει και αρκεί να αποκτήσει $k - 1$ κορίτσια ακολουθούμενα από ένα αγόρι.

Η ανεξαρτησία όμως των γεννήσεων συνεπάγεται ότι τα ενδεχόμενα $G_1, G_2, \ldots, G_{k-1}, B_k$ είναι ανεξάρτητα αφού κάθε ένα από αυτά εξαρτάται κι από διαφορετικό πείραμα. Άρα

$$\mathbf{Pr}[A_k] = \mathbf{Pr}[G_1]\mathbf{Pr}[G_2]\cdots\mathbf{Pr}[G_{k-1}]\mathbf{Pr}[B_k] = 2^{-k}.$$

Ποια η πιθανότητα τώρα του ενδεχομένου A_∞, του να αποκτήσει δηλ. η οικογένεια άπειρα παιδιά, ή, ισοδύναμα, να μην αποκτήσει ποτέ αγόρι; Είναι φανερό ότι για κάθε $k \in \mathbb{N}$ έχουμε

$$A_\infty \subseteq G_1 \cap G_2 \cap \cdots \cap G_k. \tag{11.13}$$

Αυτός ο εγκλεισμός ενδεχομένων δε λέει τίποτε άλλο από το ότι αν γνωρίζουμε ότι ισχύει το A_∞ τότε οι k πρώτες γέννες είναι κορίτσια, και αυτό φυσικά ισχύει για κάθε $k \in \mathbb{N}$. Όμως, το ενδεχόμενο στο δεξί μέρος της (11.13) έχει πιθανότητα 2^{-k} λόγω ανεξαρτησίας, άρα, για κάθε $k \in \mathbb{N}$, ισχύει $\mathbf{Pr}[A_\infty] \leq 2^{-k}$, πράγμα που μπορεί να συμβεί μόνο αν $\mathbf{Pr}[A_\infty] = 0$.

Παράδειγμα 11.16
Ρίχνουμε ένα ζάρι 10 φορές. Ποια η πιθανότητα ότι θα έρθει ακριβώς ένα 6;

Έστω E το ενδεχόμενο να μας έρθει ακριβώς ένα 6, και E_i, $i = 1, \ldots, 10$, το ενδεχόμενο να μας έρθει ακριβώς ένα έξι και μάλιστα στη θέση i. Προφανώς τα E_i αποτελούν διαμέριση του E, οπότε $\mathbf{Pr}[E] = \sum_{i=1}^{10} \mathbf{Pr}[E_i]$.

Ορίζουμε τα ενδεχόμενο A_i^k, για $k = 1, \ldots, 6$, να σημαίνει ότι στην i-οστή ρίψη το αποτέλεσμα είναι k. Προφανώς ισχύει

$$E_i = (A_1^6)^c \cap (A_2^6)^c \cap \cdots \cap A_i^6 \cap (A_{i+1}^6)^c \cap \cdots \cap (A_{10}^6)^c = A_i^6 \cap \bigcap_{j\neq i} (A_j^6)^c. \tag{11.14}$$

Για να ισχύει δηλ. το E_i πρέπει σε όλες τις ρίψεις να μη φέρουμε 6 εκτός από την i-οστή ρίψη στην οποία πρέπει να φέρουμε 6. Τα ενδεχόμενα που εμφανίζονται στο δεξί μέλος της (11.14) είναι ανεξάρτητα μια και το καθένα από αυτά αφορά διαφορετική ρίψη, άρα

$$\mathbf{Pr}[E_i] = \left(\frac{5}{6}\right)^9 \frac{1}{6},$$

αφού το ενδεχόμενα A_j^6 έχει πιθανότητα 1/6 και τα ενδεχόμενα $(A_j^6)^c$ έχουν τη συμπληρωματική πιθανότητα 5/6, για κάθε j.

Τέλος $\mathbf{Pr}[E] = \sum_{i=1}^{10} \mathbf{Pr}[E_i] = 10\left(\frac{5}{6}\right)^9 \frac{1}{6}$.

✏ **11.29**
Αποδείξτε ότι ο αριθμός $10\left(\frac{5}{6}\right)^9 \frac{1}{6}$ είναι ≤ 1 χωρίς να κάνετε καμία πράξη.

Παράδειγμα 11.17
Ρίχνουμε ένα τίμιο ζάρι άπειρες φορές. Παίρνουμε έτσι ως αποτέλεσμα του πειράματος μια άπειρη ακολουθία X_n, $n = 1, 2 \ldots$, με $X_n \in \{1, \ldots, 6\}$. Ποια η πιθανότητα να μη φέρουμε ποτέ 6; Ας είναι E το ενδεχόμενο αυτό.

Ας ονομάσουμε E_i, $i = 1, 2, \ldots$, το ενδεχόμενο να μη φέρουμε 6 στην i-οστή ρίψη. Ισχύει φυσικά $\mathbf{Pr}[E_i] = 5/6$ για κάθε ίνα μη φέρουμε ποτέ 6;

Ας ονομάσουμε E_i, $i = 1, 2, \ldots$, το ενδεχόμενο να μη φέρουμε 6 στην i-οστή ρίψη. Ισχύει φυσικά $\mathbf{Pr}[E_i] = 5/6$ για κάθε i. Επίσης η ακολουθία E_i είναι ανεξάρτητη αφού κάθε E_i αναφέρεται σε διαφορετική ρίψη. Τέλος $E = \bigcap_{i=1}^{\infty} E_i$, οπότε

$$\mathbf{Pr}[E] = \prod_{i=1}^{\infty}(5/6) = \lim_{N\to\infty}\prod_{i=1}^{N}(5/6) = \lim_{N\to\infty}(5/6)^N = 0,$$

αφού $\lim_{N\to\infty} \alpha^N = 0$ αν (και μόνο αν) $|\alpha| < 1$.

Παράδειγμα 11.18
Όπως και προηγουμένως ρίχνουμε ένα ζάρι άπειρες φορές και παίρνουμε μια άπειρη ακολουθία X_n, $n = 1, 2 \ldots$, με $X_n \in \{1, \ldots, 6\}$. Ποια η πιθανότητα να μη δούμε ποτέ στην ακολουθία αυτή τον αριθμό 1, ακολουθούμενο από τον 2, ακολουθούμενο από τον 3; (Σε διαφορετική γλώσσα ποια η πιθανότητα η λέξη 123 να μην είναι υπολέξη της άπειρης σε μήκος λέξης $X_1X_2X_3\cdots$;) Ας ονομάσουμε E αυτό το ενδεχόμενο του οποίου την πιθανότητα θέλουμε να υπολογίσουμε.

Ορίζουμε πάλι E_i να είναι το ενδεχόμενο $(X_i, X_{i+1}, X_{i+2}) \neq (1, 2, 3)$, το ενδεχόμενο δηλ. να μην εμφανιστεί η «απογορευμένη λέξη» αρχίζοντας από την i-οστή θέση της ακολουθίας. Προφανώς ισχύει και πάλι $E = \bigcap_{i=1}^{\infty} E_i$. Η ουσιαστική διαφορά με προηγουμένως είναι ότι τα E_i δεν αποτελούν πλέον ανεξάρτητη ακολουθία, τουλάχιστον όχι αν δεν το αποδείξουμε, αφού, για παράδειγμα το E_i και E_{i+1} ανεφέρονται και τα δύο στη ρίψη υπ' αριθμόν $i + 1$.

Ο τρόπος να δείξουμε και πάλι ότι $\mathbf{Pr}[E] = 0$ είναι να παρατηρήσουμε ότι τα ενδεχόμενα E_{3i}, $i = 1, 2, \ldots$, είναι ανεξάρτητα, αφού αναφέρονται σε διαφορετικά πειράματα και ότι

$$E \subseteq \bigcap_{i=1}^{\infty} E_{3i}.$$

Επίσης είναι φανερό ότι η ποσότητα E_{3i} είναι ανεξάρτητη του i και μικρότερη του 1, έστω p. Τότε $\mathbf{Pr}[E] \leq \prod_{i=1}^{\infty} \mathbf{Pr}[E_{3i}] = \prod_{i=1}^{\infty} p = 0$.

✏ **11.30**
Υπολογίστε την ποσότητα p στο Παράδειγμα 11.18.

✏ **11.31**
Γενικεύστε το Παράδειγμα 11.18 και δείξτε ότι αν X_n είναι μια ακολουθία τέτοια ώστε το X_n έχει επιλεγεί τυχαία (ας πούμε με την ομοιόμορφη κατανομή) από το σύνολο $\{1, \ldots, K\}$ ανεξάρτητα από τα άλλα X_n, και αν $w_1, w_2, \cdots, w_n \in \{1, \ldots, K\}$ είναι κάποια προεπιλεγμένα στοιχεία, τότε η πιθανότητα ότι τα στοιχεία αυτά δεν εμφανίζονται ποτέ στην ακολουθία X_n το ένα μετά το άλλο, είναι 0.

✏ **11.32**
Έστω $0 \leq a_n \leq 1$ ακολουθία αριθμών. Δείξτε ότι

$$0 = \prod_{i=1}^{\infty} a_n = \lim_{N\to\infty} \prod_{i=1}^{N} a_n$$

αν και μόνο αν $\sum_{i=1}^{\infty}(1 - a_n) = \infty$.
Πάρτε λογαρίθμους και χρησιμοποιήστε την ανισότητα

$$2(x - 1) \leq \log x \leq x - 1,$$

που ισχύει για $\theta \leq x \leq 1$ (θ είναι κάποιος αριθμός στο (0,1) που δε χρειάζεται να τον γνωρίζουμε ακριβώς).

✏ **11.33**
Ας είναι E_n μια ανεξάρτητη ακολουθία ενδεχομένων με $\sum_{n=1}^{\infty} \mathbf{Pr}[E_n] = \infty$. Δείξτε ότι σχεδόν σίγουρα ισχύουν άπειρα από τα E_n.
Χρησιμοποιήστε την Άσκηση 11.32

Παρατήρηση 11.9
Η Άσκηση 11.17 μαζί με την Άσκηση 11.33 αποτελούν το λεγόμενο Λήμμα Borel-Cantelli.

✏ **11.34**
Το καλοκαίρι έχει σχεδόν τελειώσει για τον πολύ κόσμο κι εσάς σας έχει μόλις προσλάβει μια σοβαρή

εταιρεία δημοσκοπήσεων. Ένας μεγάλος πελάτης αυτής της εταιρείας ενδιαφέρεται να εκτιμήσει το ποσοστό του κόσμου που έχει απατήσει το/η σύντροφό του το καλοκαίρι που μας πέρασε.

Η εταιρεία δημοσκοπήσεων έχει μεγάλο πρόβλημα να πραγματοποιήσει αυτή τη δημοσκόπηση. Αν η εταιρεία μπορούσε να μαζέψει ένα τυχαίο δείγμα του κόσμου, π.χ. 10.000 άτομα, σε ένα χώρο, θα μπορούσε εύκολα να τους μοιράσει ανώνυμα ερωτηματολόγια. Οι ερωτούμενοι τότε, καλυπτόμενοι από την ανωνυμία, δε θα είχαν λόγο να απαντήσουν ψέματα και από τις απαντήσεις τους θα προέκυπτε εύκολα η εκτίμηση της πιθανότητας απιστίας.

Όμως το να μαζέψει τόσο κόσμο είναι πολύ ακριβό και αυτή η μέθοδος είναι ανεφάρμοστη. Η εταιρεία δημοσκοπήσεων μπορεί όμως να βγάλει συνεργάτες της έξω οι οποίοι θα μπορούν να σταματάνε τυχαία κόσμο στο δρόμο (ή να επισκέπτονται κόσμο τυχαία στα σπίτια ή τις δουλειές τους) και να τους ρωτάνε. Και πάλι βέβαια, αν σας σταματήσει κάποιος στο δρόμο και σας κάνει τέτοια ερώτηση υπάρχει μεγάλη πιθανότητα ότι δε θα πείτε την αλήθεια (που ξέρετε αν αυτός που σας ρωτάει σας ξέρει ή όχι, κλπ).

Προτείνετε ένα τρόπο να συλλέξετε δεδομένα που θα σας οδηγήσουν στη σωστή εκτίμηση της πιθανότητας απιστίας. Πιο συγκεκριμένα, προτείνετε ένα τρόπο να απαντάει το τυχαίο άτομο μ' ένα ΝΑΙ ή ΟΧΙ, χρησιμοποιώντας κι ένα νόμισμα το οποίο μπορεί να ρίχνει όσες φορές θέλει και του οποίου το αποτέλεσμα μόνο αυτό το άτομο ξέρει. Από τις απαντήσεις αυτές θα πρέπει να μπορείτε να συνάγετε την εκτίμηση της πιθανότητας αλλά δε θα μπορείτε να βγάλετε συμπέρασμα για τις καλοκαιρινές δραστηριότητες κανενός ερωτούμενου. Επίσης αυτό το τελευταίο θα πρέπει να είναι προφανές στους ερωτούμενους.

Υποθέτουμε ότι οι ερωτούμενοι δρουν καλόπιστα και ακολουθούν τις οδηγίες σας.

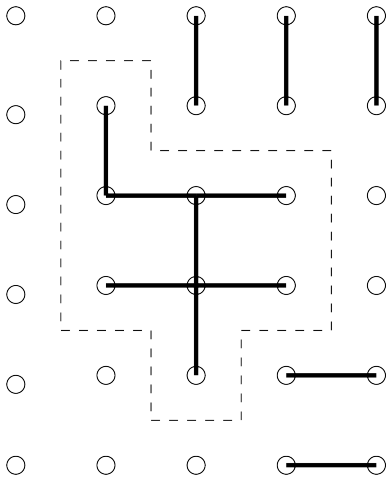
✏ **11.35**

Έστω ότι $f(x_1, \ldots, x_n)$ είναι ένα πολυώνυμο, βαθμού $\leq d$ σε κάθε μεταβλητή, και $S \subseteq \mathbb{R}$ είναι ένα πεπερασμένο σύνολο.

Επιλέγουμε τους τυχαίους αριθμούς $X_1, \ldots, X_n \in S$ ομοιόμορφα και ανεξάρτητα από το S. Δείξτε ότι

$$\mathbf{Pr}\left[f(X_1, \ldots, X_n) = 0\right] \leq \frac{d}{|S|}.$$

Επαγωγή ως προς n. Μη ξεχνάτε ότι ένα πολυώνυμο μιας μεταβλητής δε μπορεί να έχει περισσότερες ρίζες απ' ό,τι ο βαθμός του.



Σχήμα 11.1: Η συνδεσμολογία της Άσκησης 11.36

✏ **11.36**

Σε ένα $N \times N$ πίνακα από κουκίδες όλες οι κουκίδες είναι αρχικά ενωμένες με τις 4 γειτονικές τους με ακμές (εκτός από αυτές που είναι στα σύνορα οι οποίες ενώνονται με λιγότερες). Για κάθε μια από τις ακμές που υπάρχουν στην αρχή ρίχνουμε ανεξάρτητα ένα νόμισμα που έρχεται κορώνα με πιθανότητα p, ίδια για όλες τις ακμές, και αν το νόμισμα έρθει γράμματα σβήνουμε την ακμή. (Δείτε το Σχήμα 11.1.)

Θεωρήστε το ενδεχόμενο E μετά από τις διαγραφές ακμών να υπάρχει μονοπάτι που ξεκινάει από κάποια κουκίδα της αριστερής μεριάς και καταλήγει σε κάποια κουκίδα της δεξιάς μεριάς του πίνακα (το μονοπάτι αποτελείται από ακμές που δε σβήστηκαν).

Αποδείξτε ότι η πιθανότητα του E είναι αύξουσα συνάρτηση του p.

Η δυσκολία σε αυτό το πρόβλημα έγκειται στο ότι προσπαθούμε να συγκρίνουμε δύο πιθανότητες που εμφανίζονται σε δύο διαφορετικά πειράματα (με μια τιμή του p και με μια μεγαλύτερη τιμή του p). Προσπαθήστε με κάποιο τρόπο να εκφράσετε αυτά τα δύο ενδεχόμενα ως ενδεχόμενα του ίδιου πειράματος.

11.5 Video Κεφαλαίου

11.1
Πειράματα και δυνατά αποτελέσματα (video και συνοδευτικές ερωτήσεις, 4:00 λεπτά).

11.2
Πιθανότητες αποτελεσμάτων (video και συνοδευτικές ερωτήσεις, 8:48 λεπτά).

11.3
Πιθανότητες ενδεχομένων (video και συνοδευτικές ερωτήσεις, 8:24 λεπτά).

11.4
Συνολοσυνάρτηση πιθανότητας (video και συνοδευτικές ερωτήσεις, 8:24 λεπτά).

11.5
Συνολοσυνάρτηση πιθανότητας: ιδιότητες (video και συνοδευτικές ερωτήσεις, 8:24 λεπτά).

11.6
Ρίψη δύο ζαριών. (video και συνοδευτικές ερωτήσεις, 7:24 λεπτά).

11.7
Ρίψη δύο ζαριών: κάποια ενδεχόμενα. (video και συνοδευτικές ερωτήσεις, 5:04 λεπτά).

11.8
Παράδειγμα: ρίψη n νομισμάτων. (video και συνοδευτικές ερωτήσεις, 10:45 λεπτά).

11.9
Παράδειγμα: ρίψη n νομισμάτων. Κάποια ενδεχόμενα. (video και συνοδευτικές ερωτήσεις, 9:51 λεπτά).

11.10
Παράδειγμα: Κάνουμε παιδιά μέχρι να κάνουμε αγόρι. (video και συνοδευτικές ερωτήσεις, 9:36 λεπτά).

11.11
liminf και limsup ενδεχομένων. (video και συνοδευτικές ερωτήσεις, 13:30 λεπτά).

11.12
Ακολουθία ενδεχομένων με πεπερασμένη συνολικά πιθανότητα. (video και συνοδευτικές ερωτήσεις, 8:39 λεπτά).

11.13
Υπό συνθήκη πιθανότητα. (video και συνοδευτικές ερωτήσεις, 6:49 λεπτά).

11.14
Υπό συνθήκη πιθανότητα: παραδείγματα. (video και συνοδευτικές ερωτήσεις, 8:39 λεπτά).

11.15
Τύπος ολικής πιθανότητας. (video και συνοδευτικές ερωτήσεις, 9:58 λεπτά).

11.16
Τύπος του Bayes. (video και συνοδευτικές ερωτήσεις, 10:45 λεπτά).

11.17
Ανεξαρτησία ενδεχομένων: παραδείγματα. (video και συνοδευτικές ερωτήσεις, 14:27 λεπτά).

11.18
Ανεξαρτησία πολλών ενδεχομένων. (video και συνοδευτικές ερωτήσεις, 7:34 λεπτά).

11.19
Ρίψεις δύο νομισμάτων και κατανομή. (video και συνοδευτικές ερωτήσεις, 5:47 λεπτά).

11.20
Δύο ασύμμετρα ζάρια. (video και συνοδευτικές ερωτήσεις, 22:28 λεπτά).

11.21
Το παράδοξο των γενεθλίων. (video και συνοδευτικές ερωτήσεις, 11:35 λεπτά).

Βιβλιογραφία Κεφαλαίου

[1] Charles Miller Grinstead and James Laurie Snell. *Introduction to probability*. American Mathematical Soc., 2012.

[2] Paul Gerhard Hoel, Sidney C Port, and Charles J Stone. *Introduction to probability theory*. Vol. 12. Houghton Mifflin Boston, 1971.

[3] Sheldon Ross. *A first course in probability*. Macmillan, New York, NY, 1976.

Κεφάλαιο 12

Τυχαίες μεταβλητές και μέση τιμή

Κύριες βιβλιογραφικές αναφορές για αυτό το Κεφάλαιο είναι οι Ross 1976, Grinstead and Snell 2012 και Hoel, Port, and Stone 1971.

12.1 Τυχαίες μεταβλητές και η κατανομή τους

Παράδειγμα 12.1
Ας υποθέσουμε ότι ρίχνουμε δύο φορές ένα συνηθισμένο ζάρι, και συμβολίζουμε με X_1 το αποτέλεσμα της 1ης ρίψης ($X_1 \in \{1, \ldots, 6\}$) και X_2 το αποτέλεσμα της 2ης ρίψης. Ορίζουμε ακόμη $X = X_1 + X_2$ να είναι το άθροισμα των δύο ρίψεων. Οι ποσότητες X, X_1, X_2 εν γένει αλλάζουν κάθε φορά που πραγματοποιείται το πείραμα. Τέτοιες ποσότητες, των οποίων η τιμή εξαρτάται από την έκβαση κάποιου πειράματος, τις ονομάζουμε τυχαίες μεταβλητές.

Ορισμός 12.1
(Τυχαία μεταβλητή) *Αν Ω είναι δειγματικός χώρος ενός πειράματος ονομάζουμε Τυχαία Μεταβλητή (ΤΜ) πάνω στο Ω κάθε συνάρτηση πάνω στο Ω. Αν $X : \Omega \to \mathbb{R}$ ή $X : \Omega \to \mathbb{Z}$ θα ονομάζουμε ειδικότερα την ΤΜ X* αριθμητική ΤΜ *ενώ αν $X : \Omega \to \mathbb{R}^d$ ή $X : \Omega \to \mathbb{Z}^d$ θα ονομάζουμε την X* πολυδιάστατη *ή* διανυσματική *ΤΜ.*

Αν $X : \Omega \to T$ και το σύνολο τιμών T είναι πεπερασμένο ή αριθμήσιμο τότε η ΤΜ X ονομάζεται διακριτή.

Αριθμήσιμο ονομάζεται ένα σύνολο A αν υπάρχει επί συνάρτηση $f : \mathbb{N} \to A$ από το σύνολο των φυσικών αριθμών επί του A. Με άλλα λόγια, το A είναι αριθμήσιμο αν μπορούμε να βρούμε μια ακολουθία $a_1, a_2, \ldots$ που περιέχει όλα τα στοιχεία του.

Είναι προφανές ότι κάθε πεπερασμένο σύνολο είναι αριθμήσιμο. Επίσης αριθμήσιμα σύνολα είναι οι φυσικοί αριθμοί $\mathbb{N}$, οι ακέραιοι $\mathbb{Z}$, οι ρητοί $\mathbb{Q}$, καρτεσιανά γινόμενα $A \times B$, όπου τα A και B είναι αριθμήσιμα, και άπειρες ενώσεις του τύπου $\bigcup_{j=1}^{\infty} A_j$, όπου τα A_j είναι αριθμήσιμα.

Σύνολα που δεν είναι αριθμήσιμα είναι π.χ. το $\mathbb{R}$ ή ένα διάστημα (a, b), $a < b$. Αυτό το τελευταίο δεν είναι προφανές και θέλει απόδειξη, την οποία δε θα δώσουμε εδώ.

Μπορείτε επίσης να συμβουλευτείτε την §1.8 αυτών των σημειώσεων.

Παρατήρηση 12.1
Εύκολα βλέπει κανείς (χρησιμοποιώντας το γεγονός ότι καρτεσιανά γινόμενα αριθμησίμων συνόλων με πεπερασμένους σε πλήθος παράγοντες είναι επίσης αριθμήσιμα) ότι αν $X_1, \ldots, X_n$ είναι διακριτές ΤΜ και $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ τότε η ΤΜ $Z = \lambda_1 X_1 + \cdots + \lambda_n X_n$ είναι επίσης διακριτή. Έτσι μπορούμε ελεύθερα να μιλάμε για πεπερασμένους γραμμικούς συνδυασμούς διακριτών ΤΜ γνωρίζοντας εκ των προτέρων ότι κι αυτοί είναι διακριτές ΤΜ.

Κάτι τέτοιο δεν ισχύει για άπειρους γραμμικούς συνδυασμούς από ΤΜ. Για παράδειγμα, αν X_j, $j = 1, 2, \ldots$, είναι ΤΜ τέτοιες ώστε η X_j έχει σύνολο τιμών το $\{0, 2^{-j}\}$, τότε η ΤΜ $Z = \sum_{j=1}^{\infty} X_j$ ορίζεται χωρίς πρόβλημα αφού η σειρά πάντα συγκλίνει, ότι τιμές και να έχουν τα X_j, αλλά μπορεί εν δυνάμει

(για παράδειγμα όταν όλες οι X_j είναι ανεξάρτητες – δείτε παρακάτω τον Ορισμό 12.4 για τον ορισμό της ανεξαρτησίας ΤΜ) να πάρει οποιονδήποτε πραγματικό αριθμό του διαστήματος $(0,1)$ ως τιμή. Πράγματι, αν $x \in (0,1)$ τότε, γράφοντας τον x στο δυαδικό του ανάπτυγμα $x = \sum_{j=1}^{\infty} x_j 2^{-j}$, με $x_j \in \{0,1\}$, βλέπουμε ότι είναι δυνατό να έχουμε $Z = x$ φτάνει να πάρουν οι X_j τις κατάλληλες τιμές.

Παράδειγμα 12.2
Στο Παράδειγμα 12.1 οι ΤΜ που ορίσαμε είναι όλες αριθμητικές και διακριτές. Η ΤΜ $Z = (X_1, X_2)$ έχει σύνολο τιμών το $\{1,\ldots,6\}^2$ και είναι διανυσματική ΤΜ.

Παράδειγμα 12.3
Ας υποθέσουμε ότι παρατηρούμε μια καταιγίδα και καταγράφουμε τη χρονική στιγμή που θα πέσει η πρώτη αστραπή. Η ΤΜ αυτή (χρόνος) είναι μια αριθμητική αλλά όχι διακριτή ΤΜ αφού το σύνολο τιμών είναι το διάστημα $[0,\infty)$.

Παράδειγμα 12.4
Ρίχνουμε ένα νόμισμα (που φέρνει κορώνα με πιθανότητα $p \in (0,1)$) άπειρες φορές και έστω X η πρώτη φορά που έρχεται κορώνα. Αυτή η ΤΜ έχει το $\{1,2,\ldots\}$ ως σύνολο τιμών και είναι άρα διακριτή, αριθμητική ΤΜ.

Παρατήρηση 12.2
Αν έχουμε μια ΤΜ που παίρνει τιμές σε ένα μη αριθμητικό σύνολο, π.χ. μια ΤΜ που παίρνει τιμές Κ ή Γ (το αποτέλεσμα της ρίψης ενός νομίσματος), θα κωδικοποιούμε συνήθως τις τιμές αυτές με φυσικούς αριθμούς, για παράδειγμα 1 αντί Κ και 0 αντί Γ, ώστε να θεωρούμε ότι οι ΤΜ αυτές παίρνουν αριθμητικές τιμές.

Σε μερικές περιπτώσεις όμως αυτό είναι αρκετά αφύσικο. Για παράδειγμα αν έχουμε μια ΤΜ που παίρνει ρητές τιμές, μπορούμε φυσικά να κάνουμε αυτή την κωδικοποίηση που σε κάθε ρητό αντιστοιχεί ένα ακέραιο, όμως αυτή η διαδικασία στερείται φυσικότητας και, κατά κανόνα, δεν πρόκειται να προσφέρει τίποτα στην ανάλυση.

Πάνω στο δειγματικό χώρο Ω υπάρχει ορισμένη η κατανομή πιθανότητας (δείτε Ορισμό 11.2), μια συνάρτηση δηλ. $p : \Omega \to [0,1]$, τ.ώ. η τιμή $p(\omega)$ μας δηλώνει πόσο πιθανό είναι το αποτέλεσμα ω όταν εκτελεσθεί το πείραμα. Αν τώρα $X : \Omega \to T$ (T ένα οποιοδήποτε σύνολο τιμών) είναι μια ΤΜ X με τιμές στο T, μπορούμε τότε να θεωρήσουμε ένα νέο πείραμα με αποτέλεσμα $X(\omega)$. Εκτελούμε δηλ. το προηγούμενο πείραμα (αυτό με δειγματικό χώρο Ω), μας δίνει αυτό κάποιο αποτέλεσμα $\omega \in \Omega$, και αναφέρουμε ως αποτέλεσμα του νέου μας πειράματος το $X(\omega) \in T$. Το νέο αυτό πείραμα έχει το T ως δειγματικό χώρο και μια νέα κατανομή πιθανότητας $p : T \to [0,1]$ που ορίζεται από

$$p(t) = \mathbf{Pr}\left[\omega : X(\omega) = t\right].$$

Οι πιθανοθεωρητικές ερωτήσεις λοιπόν που αφορούν την ΤΜ X λοιπόν μπορούν να μελετηθούν πάνω σε αυτόν τον νεό δειγματικό χώρο T, σύνολο τιμών της X. Έχει επικρατήσει όμως συχνά να μην αναφερόμαστε στο νέο αυτό δειγματικό χώρο και να μελετάμε τέτοια ερωτήματα πάνω στον παλιό δειγματικό χώρο Ω. Ο κυριότερος λόγος γι' αυτό είναι ότι πολύ συχνά μελετάμε παραπάνω από μια ΤΜ και μάλιστα σε συνδυασμό, οπότε αν περιοριστεί κανείς στο δειγματικό χώρο T για μια από τις ΤΜ αυτές, πράξη που πάντα συνεπάγεται «χάσιμο πληροφορίας», δε μπορεί να μελετήσει τις άλλες.

Ορισμός 12.2
(Πυκνότητα πιθανότητας) *Αν X είναι μια διακριτή ΤΜ με σύνολο τιμών T τότε ονομάζουμε* πυκνότητα πιθανότητας *της X τη συνάρτηση $f_X : T \to [0,1]$ που δίδεται από τον τύπο*

$$f_X(t) = \mathbf{Pr}\left[X = t\right].$$

Για μια οποιαδήποτε (διακριτή ή όχι) ΤΜ X με τιμές στο $\mathbb{R}$ ορίζουμε τη συνάρτηση κατανομής *της X ως τη συνάρτηση $F_X : \mathbb{R} \to [0,1]$ που δίδεται από τον τύπο*

$$F_X(x) = \mathbf{Pr}\left[X \le x\right].$$

Παρατήρηση 12.3
Η συνάρτηση κατανομής F_X είναι μια αύξουσα συνάρτηση (όχι κατ' ανάγκη γνήσια αύξουσα) τέτοια ώστε $\lim_{k\to-\infty} F_X(k) = 0$ *και* $\lim_{k\to\infty} F_X(k) = 1$.

Είναι επίσης προφανές ότι αν $X \in \mathbb{Z}$ τότε για κάθε $n \in \mathbb{Z}$ έχουμε

$$F_X(n) = \sum_{k=-\infty}^{n} f_X(k). \tag{12.1}$$

Τέλος, $\sum_{n=-\infty}^{\infty} f_X(n) = 1$.

Παρατήρηση 12.4
Η συνάρτηση κατανομής της X ορίζεται για κάθε πραγματικό x ακόμα κι αν είναι γνωστό εκ των προτέρων ότι η X παίρνει μόνο ακέραιες τιμές. Σε αυτή βέβαια την περίπτωση ισχύει $F_X(x) = F_X(\lfloor x \rfloor)$ οπότε αρκεί να μελετήσει κανείς την F_X για ακέραιες μόνο τιμές της μεταβλητής.

Ορισμός 12.3
(Ισόνομες τυχαίες μεταβλητές) *Δύο ΤΜ X και Y λέγονται ισόνομες αν έχουν την ίδια συνάρτηση κατανομής.*

Παρατήρηση 12.5
Δύο ΤΜ X και Y είναι ίσες αν και μόνο αν $X(\omega) = Y(\omega)$ για κάθε $\omega \in \Omega$. Δηλ. για κάθε έκβαση του πειράματος οι X και Y έχουν την ίδια τιμή. Αυτή είναι πολύ ισχυρή έννοια. Αντίθετα, δύο ΤΜ είναι ισόνομες αν έχουν απλά (αν πρόκειται για διακριτές μεταβλητές) την ίδια πυκνότητα. Για παράδειγμα, αν κρατάμε δύο ίδια ζάρια στα χέρια μας και ονομάσουμε X το αποτέλεσμα του πρώτου και Y του δεύτερου, τότε οι X και Y είναι φυσικά ισόνομες αλλά δεν είναι ίσες αφού σε κάποια πειράματα θα εμφανίσουν διαφορετικές τιμές.

Παράδειγμα 12.5
Αν $X \in \{K, \Gamma\}$ είναι το αποτέλεσμα της ρίψης ενός ζαριού που φέρνει κορώνα με πιθανότητα $p \in (0,1)$ τότε η πυκνότητα πιθανότητας της X είναι η συνάρτηση $f_X : \{K, \Gamma\} \to [0,1]$ που δίνεται από τις τιμές $f_X(K) = p$, $f_X(\Gamma) = 1 - p$.

Παράδειγμα 12.6
Αν $X \in \mathbb{Z}$ είναι το αποτέλεσμα της ρίψης ενός ζαριού τότε

$$f_X(n) = \begin{cases} 1/6 & n \in \{1, \ldots, 6\} \\ 0 & \alpha\lambda\lambda\iota\omega\varsigma \end{cases},$$

και εύκολα βλέπουμε ότι $F_X(n)$ ισούται με 0 για $n \le 0$, $F_X(n) = 1$ για $n \ge 6$ και $F_X(n) = n/6$ για $n \in \{1, 2, \ldots, 6\}$.

Παράδειγμα 12.7
Αν $X \in \mathbb{Z}$ είναι το αποτέλεσμα της ρίψης ενός ζαριού και $Y = X^2$ τότε

$$f_Y(n) = \begin{cases} 1/6 & n \in \{1, 2^2, \ldots, 6^2\} \\ 0 & \alpha\lambda\lambda\iota\omega\varsigma \end{cases}.$$

Επίσης $F_Y(n)$ ισούται με 0 για $n \le 0$, $F_Y(n) = 1$ για $n \ge 36$ και $F_Y(n) = \lfloor\sqrt{n}\rfloor/6$ για $n \in \{1, 2, \ldots, 36\}$.

Παράδειγμα 12.8
Αν A είναι ένα οποιοδήποτε ενδεχόμενο η ΤΜ $X(\omega) = \mathbf{1}(\omega \in A)$ ονομάζεται δείκτρια ΤΜ του ενδεχομένου A και παίρνει τιμή 1 αν ισχύει το A, 0 αλλιώς. Η πυκνότητα πιθανότητας της A παίρνει την τιμή $\mathbf{Pr}[A]$ *στον αριθμό 1,* $1 - \mathbf{Pr}[A]$ *στον αριθμό* 0*, και 0 παντού αλλού.*

✏ **12.1**
Η συνάρτηση $\Omega \to \mathbb{R}$ που είναι ίση με c παντού ονομάζεται σταθερή ΤΜ με τιμή c. Ποια η πυκνότητα πιθανότητάς της και ποια η συνάρτηση κατανομής της;

Παράδειγμα 12.9
Λέμε ότι η ΤΜ X είναι ομοιόμορφα κατανεμημένη *στο (πεπερασμένο) σύνολο T αν η ποσότητα $\mathbf{Pr}[X = t]$ δεν εξαρτάται από το $t \in T$. Αυτό σημαίνει ότι η πυκνότητα πιθανότητας είναι ίση με $1/|T|$ σε κάθε στοιχείο του T.*

✏ **12.2**
Αν X είναι ομοιόμορφα κατανεμημένη στο $[n]$ και $Y = 2^X$ περιγράψτε τις συναρτήσεις f_Y και F_Y.

✏ **12.3**
Η ΤΜ $X \in \mathbb{Z}$ έχει πυκνότητα πιθανότητας f_X. Γράψτε από ένα άθροισμα τιμών της f_X που να δίνει την πιθανότητα των παρακάτω ενδεχομένων:

1. $\{X \leq 0\}$
2. $\{X\ \alpha\rho\tau\iota o\}$
3. $\{|X| \leq 100\}$.

✏ **12.4**
Αν $Y = -X + b$, b σταθερά, δώστε ένα τύπο για τις f_Y, F_Y, μέσω των f_X, F_X.

Παράδειγμα 12.10
Ένα νόμισμα φέρνει κορώνα με πιθανότητα $p \in (0, 1)$. Το ρίχνουμε άπειρες φορές και έστω X η ρίψη κατά την οποία εμφανίζεται η πρώτη κορώνα. Είναι φανερό ότι $X \in \{1, 2, \ldots\} \cup \{\infty\}$, αφού μπορεί κατά τη διάρκει του πειράματος να μην εμφανιστεί ποτέ κορώνα. (Το ότι χρησιμοποιήσαμε το σύμβολο ∞ για να δηλώσουμε ότι δεν έρχεται ποτέ κορώνα κατά κάποια εκτέλεση του πειράματος πρόκειται απλά για μια σύμβαση και δεν έχει τίποτε να κάνει με τις ιδιότητες μεγέθους που δίδει κανείς συνήθως στο σύμβολο ∞, π.χ. ότι είναι μεγαλύτερο από κάθε φυσικό αριθμό. Θα μπορούσαμε δηλ. εξίσου καλά να δίδαμε τιμή $X = 0$ ή $X =$«ΠΟΤΕ» στην περίπτωση αυτή.) Ας είναι $X_i = 1$ αν το νόμισμα φέρει κορώνα στην i-οστή ρίψη και $X_i = 0$ αν φέρει γράμματα. Έχουμε, για $n = 1, 2, \ldots$,

$$f_X(n) = \mathbf{Pr}[X = n] = \mathbf{Pr}[X_1 = 0, X_2 = 0, \ldots, X_{n-1} = 0, X_n = 1],$$

και, λόγω της ανεξαρτησίας των ενδεχομένων $\{X_1 = 0\}, \ldots, \{X_{n-1} = 0\}, \{X_n = 1\}$,

$$f_X(n) = \mathbf{Pr}[X_1 = 0] \cdots \mathbf{Pr}[X_{n-1} = 0] \cdot \mathbf{Pr}[X_n = 1] = p(1-p)^{n-1}, \tag{12.2}$$

και για κάθε $n \leq 0$ έχουμε προφανώς $f_X(n) = 0$. Τέλος επειδή $\{X = \infty\} \subseteq \{X_1 = 0, \ldots, X_k = 0\}$ για κάθε $k \geq 1$, και επειδή η πιθανότητα του δεύτερου ενδεχομένου ισούται με $(1-p)^k$, και άρα συγκλίνει στο 0 με το k, έπεται ότι

$$f_X(\infty) = \mathbf{Pr}[X = \infty] = 0.$$

Έχουμε λοιπόν προσδιορίσει πλήρως την πυκνότητα της X.

Η X δεν είναι αριθμητική ΤΜ αφού παίρνει και την τιμή ∞, οπότε δεν ορίζεται η συνάρτηση κατανομής. Όμως, μπορεί κανείς να μελετήσει την ΤΜ

$$Y = X \cdot \mathbf{1}(X\ \pi\varepsilon\pi\varepsilon\rho\alpha\sigma\mu\varepsilon\nu\eta) = \begin{cases} X & \alpha\nu\ X\ \pi\varepsilon\pi\varepsilon\rho\alpha\sigma\mu\varepsilon\nu\eta \\ 0 & \alpha\lambda\lambda\iota\omega\varsigma \end{cases},$$

που είναι σχεδόν σίγουρα ίση με την X (όσον αφορά τις πιθανοθεωρητικές τους ιδιότητες δύο ΤΜ που είναι ίσες σχεδόν σίγουρα είναι ουσιαστικά η ίδια ΤΜ και τις θεωρούμε μία) αφού $\mathbf{Pr}[X \neq Y] =$

Pr $[X = \infty] = 0$. *Γι' αυτό εφαρμόζουμε τον τύπο* (12.1). *Για* $n \leq 0$ *έχουμε φυσικά* $F_Y(n) = 0$. *Για* $n \geq 0$ *έχουμε*

$$\begin{aligned} F_Y(n) &= \sum_{k=-\infty}^{n} f_X(k) \\ &= \sum_{k=1}^{n} p(1-p)^{k-1} \\ &= p\sum_{l=0}^{n-1}(1-p)^{l} \quad \dagger \\ &= p\frac{1-(1-p)^n}{1-(1-p)} \quad \ddagger \\ &= 1-(1-p)^n \end{aligned}$$

(†: αλλαγή μεταβλητής $l = k-1$, ‡: *πεπερασμένη γεωμ. σειρά).*

Η πυκνότητα (12.2) *ονομάζεται* γεωμετρική κατανομή με παράμετρο p.

Παράδειγμα 12.11

Ας υποθέσουμε ότι X *είναι ένα τυχαίο σημείο του* $[0,1]$, *και ότι το* X *είναι ομοιόμορφα κατανεμημένο στο* $[0,1]$. *Αυτό σημαίνει ότι αν* A *και* B *είναι δύο υποσύνολα του* $[0,1]$ *με το ίδιο μήκος τότε* **Pr** $[X \in A] =$ **Pr** $[X \in B]$.

Η αριθμητική TM X *δεν είναι διακριτή, οπότε δεν ορίζουμε συνάρτηση πυκνότητας πιθανότητας. Όμως η συνάρτηση κατανομής της* X *ορίζεται και είναι πολύ εύκολο να υπολογιστεί, αφού λόγω της ομοιόμορφης κατανομής έχουμε* **Pr** $[X \in [0,x]] = x$. *Αν λοιπόν* $x \leq 0$ *τότε* $F_X(x) = 0$, *αν* $x \geq 1$ *τότε* $F_X(x) = 1$ *και αν* $0 \leq x \leq 1$ *τότε* $F_X(x) = x$.

Παράδειγμα 12.12

Ρίχνουμε N *φορές ένα νόμισμα που φέρνει κορώνα με πιθανότητα* $p \in (0,1)$ *και έστω* X *το πλήθος των φορών που το νόμισμα έρχεται κορώνα. Προφανώς* $X \in \{0,\ldots,N\}$. *Για να υπολογίσουμε το* $f_X(k) =$ **Pr** $[X = k]$, $0 \leq k \leq N$, *σκεφτόμαστε ως εξής. Έστω* $\mathcal{B}$ *το σύνολο όλων των υποσυνόλων του* $[N]$ *μεγέθους* k, *και για κάθε* $B \in \mathcal{B}$ *ορίζουμε το ενδεχόμενο*

$$E_B = \{ \text{ το νόμισμα φέρνει κορώνα τη χρονική στιγμή } t \text{ αν και μόνο αν } t \in B\}.$$

Είναι φανερό ότι τα E_B, $B \in \mathcal{B}$, *αποτελούν μια διαμέριση του ενδεχομένου* $\{X = k\}$. *Επίσης για κάθε* $B \in \mathcal{B}$ *η πιθανότητα του* E_B *ισούται με* $p^k(1-p)^{N-k}$ *αφού το* E_B *ισχύει αν και μόνο αν το νόμισμα φέρει κορώνα σε κάθε μια από τις* k *χρονικές στιγμές που ανήκουν στο* B *και γράμματα σε κάθε μια από τις υπόλοιπες* $N-k$ *χρονικές στιγμές, και τα ενδεχόμενα αυτά είναι ανεξάρτητα. Τέλος* $|E_B| = \binom{N}{k}$ *οπότε*

$$f_X(k) = \binom{N}{k} p^k(1-p)^{N-k}, \quad (0 \leq k \leq N). \tag{12.3}$$

Η συνάρτηση κατανομής $F_X(k)$ *ισούται με 0 αν* $k < 0$ *και με 1 αν* $k > N$. *Για* $0 \leq k \leq N$ *δίδεται από τον τύπο*

$$F_X(k) = \sum_{l=0}^{k} \binom{N}{l} p^l(1-p)^{N-l},$$

και δεν υπάρχει γενικά κάποια απλούστευση του τύπου αυτού.

Η πυκνότητα (12.3) *ονομάζεται* διωνυμική κατανομή με παραμέτρους p και N.

✏ **12.5**
Έχουμε n παίκτες που ρίχνουν από ένα τίμιο νόμισμα ο καθένας. Όσοι από αυτούς φέρουν κορώνα ξαναρίχνουν το νόμισμά τους και έστω X ο αριθμός αυτών που ξαναφέρνουν κορώνα. Να βρεθεί η πυκνότητα πιθανότητας της ΤΜ X.

Παράδειγμα 12.13
Αν $\lambda > 0$ είναι μια παράμετρος, η πυκνότητα

$$f(n) = e^{-\lambda}\frac{\lambda^n}{n!}\mathbf{1}\left(n \geq 0\right) \tag{12.4}$$

ονομάζεται κατανομή Poisson με παράμετρο λ. *Για να επιβεβαιώσουμε ότι η (12.4) είναι όντως μια πυκνότητα αρκεί να επικαλεστούμε τον τύπο*

$$e^x = \sum_{n\geq 0}\frac{x^n}{n!},$$

που ισχύει για κάθε $x \in \mathbb{R}$.

✏ **12.6**
Η X ακολουθεί γεωμετρική κατανομή με παράμετρο p. Βρείτε την πυκνότητα της X^2.

✏ **12.7**
Η X ακολουθεί γεωμετρική κατανομή με παράμετρο p και C είναι σταθερά. Ορίζουμε $Y = X\mathbf{1}\left(X \leq C\right) + C\mathbf{1}\left(X > C\right)$. Να βρεθεί η πυκνότητα της Y.

Ορισμός 12.4
Έστω $X_1, \ldots, X_n$ διακριτές ΤΜ πάνω σε ένα δειγματικό χώρο Ω. Αυτές λέγονται ανεξάρτητες *ΤΜ αν για κάθε $x_1, \ldots, x_n$ ισχύει*

$$\mathbf{Pr}\left[X_1 = x_1, \ldots, X_n = x_n\right] = \mathbf{Pr}\left[X_1 = x_1\right]\cdots\mathbf{Pr}\left[X_n = x_n\right].$$

Ένα άπειρο σύνολο από ΤΜ πάνω στον ίδιο δειγματικό χώρο λέγεται ανεξάρτητο *αν κάθε πεπερασμένο υποσύνολο είναι ανεξάρτητο.*

Παρατήρηση 12.6
Αν η X_i παίρνει τιμές στο σύνολο T_i τότε η διανυσματική ΤΜ $(X_1, \ldots, X_n)$ παίρνει τιμές στο $T_1 \times \cdots \times T_n$. Η ανεξαρτησία των X_i μπορεί ισοδύναμα να γραφεί ως

$$f_{(X_1,\ldots,X_n)}(t_1, \ldots, t_n) = f_{X_1}(t_1)\cdots f_{X_n}(t_n).$$

✏ **12.8**
Δείξτε ότι αν οι διακριτές ΤΜ X και Y είναι ανεξάρτητες τότε για οποιαδήποτε σύνολα A και B ισχύει $\mathbf{Pr}\left[X \in A, Y \in B\right] = \mathbf{Pr}\left[X \in A\right]\mathbf{Pr}\left[Y \in B\right]$.

✏ **12.9**
Δείξτε ότι αν οι X και Y είναι ανεξάρτητες τότε και οι $f(X)$, $g(Y)$ είναι ανεξάρτητες, όπου f και g είναι τυχούσες συναρτήσεις.

✏ **12.10**
Οι X και Y είναι ανεξάρτητες και ισόνομες και $\mathbf{Pr}\left[X = 1\right] = \mathbf{Pr}\left[X = -1\right] = 1/2$. Ορίζουμε $Z = XY$. Δείξτε ότι οι X, Y, Z είναι ανεξάρτητες ανά δύο αλλά όχι ανεξάρτητες.

✏ **12.11**
Οι X και Y είναι ανεξάρτητες και ισόνομες και $\mathbf{Pr}\left[X = k\right] = 2^{-k}$, $k = 1, 2, \ldots$. Υπολογίστε τις ποσότητες

1. $\mathbf{Pr}\left[\min\left\{X, Y\right\} \leq n\right]$,

2. **Pr** $[Y > X]$,

3. **Pr** $[X = Y]$,

4. **Pr** $[X \geq kY]$, *για δοσμένο θετικό ακέραιο* k,

5. **Pr**$[X$ *διαιρεί* $Y]$,

6. **Pr** $[X = rY]$, *για δοσμένο θετικό ρητό* r.

✏ **12.12**
Αν f *και* g *είναι συναρτήσεις* $\mathbb{Z} \to \mathbb{R}$ *με* $F = \sum_{n=-\infty}^{\infty} |f(n)| < \infty$ *και* $G = \sum_{n=-\infty}^{\infty} |g(n)| < \infty$ *δείξτε ότι το άθροισμα*

$$f * g(n) = \sum_{k=-\infty}^{\infty} f(k)g(n-k) = \sum_{k=-\infty}^{\infty} f(n-k)g(k)$$

συγκλίνει για κάθε $n \in \mathbb{Z}$ *και ότι*

$$\sum_{n=-\infty}^{\infty} |f * g(n)| \leq F \cdot G.$$

Αν $f, g \geq 0$ *τότε* $f * g \geq 0$ *και η παραπάνω ανισότητα ισχύει ως ισότητα.*

Ορισμός 12.5
(Συνέλιξη) *Έστω* $f, g : \mathbb{Z} \to \mathbb{R}$ *συναρτήσεις που ικανοποιούν* $\sum_{n=-\infty}^{\infty} |f(n)| < \infty$ *και ομοίως για την* g. *Η συνάρτηση* $f * g$ *που ορίζεται στην Άσκηση 12.12 ονομάζεται* συνέλιξη *των* f *και* g.

✏ **12.13**
Δείξτε ότι $f * g = g * f$ *και* $f * (g + h) = f * g + f * h$, *όταν όλες οι συνελίξεις ορίζονται.*

Παρατήρηση 12.7
Χρησιμοποιώντας την Άσκηση 12.12 βλέπουμε ότι αν f *και* g *είναι πυκνότητες πιθανότητας, αν δηλ. υπάρχουν ΤΜ* X *και* Y *τέτοιες ώστε* $f = f_X$ *και* $g = f_Y$, *ή, ισοδύναμα, αν για κάθε μια από τις* f *και* g *ισχύουν τα*

1. $f(n) \geq 0$, *για κάθε* $n \in \mathbb{Z}$,

2. $\sum_{n=-\infty}^{\infty} f(n) = 1$,

τότε και η συνέλιξη $f * g$ *επίσης είναι πυκνότητα πιθανότητας.*

Θεώρημα 12.1
Αν X *και* Y *είναι ανεξάρτητες ΤΜ με ακέραιες τιμές τότε*

$$f_{X+Y}(n) = f_X * f_Y(n),$$

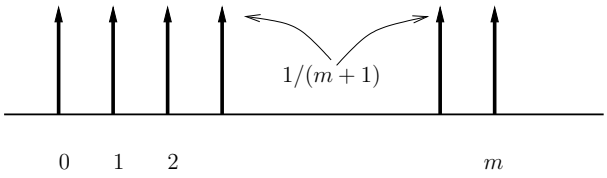
για κάθε $n \in \mathbb{Z}$.

Απόδειξη

$$\begin{aligned} f_{X+Y}(n) &= \mathbf{Pr}\left[X+Y=n\right] \\ &= \sum_{k=-\infty}^{\infty} \mathbf{Pr}\left[X+Y=n \mid Y=k\right]\mathbf{Pr}\left[Y=k\right] \quad \dagger \\ &= \sum_{k=-\infty}^{\infty} \mathbf{Pr}\left[X=n-k\right]\mathbf{Pr}\left[Y=k\right] \\ &= \sum_{k=-\infty}^{\infty} f_X(n-k) f_Y(k) \\ &= f_X * f_Y(n) \end{aligned}$$

(†: από Θεώρημα 11.3).
■

Παράδειγμα 12.14
Έστω X, Y ανεξάρτητες και ομοιόμορφες στο $\{0,\ldots,m\}$. Ποια η πυκνότητα πιθανότητας της $Z = X + Y$;



Σχήμα 12.1: Η πυκνότητα της ομοιόμορφης κατανομής στο $\{0,\ldots,m\}$

Πρέπει φυσικά να υπολογίσουμε τη συνέλιξη $f_X * f_Y$ ή $f_X * f_X$, αφού οι X και Y είναι ισόνομες (έχουν δηλ. την ίδια κατανομή). Το ότι η X είναι ομοιόμορφα κατανεμημένη στο $\{0,\ldots,m\}$ σημαίνει ακριβώς ότι

$$f_X(n) = \frac{1}{m+1}\mathbf{1}\left(0 \le n \le m\right).$$

Έχουμε λοιπόν

$$\begin{aligned} f_Z(n) &= \sum_k f_X(k) f_X(n-k) \\ &= \frac{1}{(m+1)^2}\sum_k \mathbf{1}\left(0 \le k \le m,\ 0 \le n-k \le m\right) \\ &= \frac{1}{(m+1)^2}\sum_k \mathbf{1}\left(0 \le k \le m,\ n-m \le k \le n\right) \\ &= \frac{1}{(m+1)^2}\sum_k \mathbf{1}\left(\max\left\{0, n-m\right\} \le k \le \min\left\{m, n\right\}\right) \end{aligned}$$

Παρατηρώντας ότι

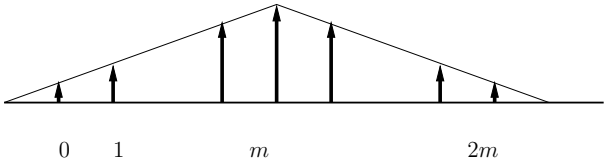
$$|\{k:\ A \le k \le B\}| = (B - A + 1)\mathbf{1}\,(A \le B)\,,$$

παίρνουμε

$$f_Z(n) = \frac{1}{(m+1)^2}(\min\{m,n\} - \max\{0, n-m\} + 1)\mathbf{1}\,(\max\{0,n-m\} \le \min\{m,n\})\,.$$

Για να βρούμε ένα πιο κατανοητό τύπο για την $f_Z(n)$ χωρίζουμε τις περιπτώσεις $n < 0$, $0 \le n \le m$, $m < n \le 2m$ και $2m < n$. Για κάθε μια από αυτές μπορούμε να υπολογίσουμε τις τιμές των $\max\{0, n-m\}, \min\{m,n\}$*, και καταλήγουμε στο αποτέλεσμα*

$$f_Z(n) = \begin{cases} 0 & n < 0 \\ \frac{n+1}{(m+1)^2} & 0 \le n \le m \\ \frac{2m-n+1}{(m+1)^2} & m < n \le 2m \\ 0 & 2m < n \end{cases}$$



Σχήμα 12.2: Η πυκνότητα της $X + Y$

✏ **12.14**
Να βρεθεί η $f_Y(n)$ μέσω της $f_X(n)$ αν $Y = X + t$, όπου t ένας σταθερός ακέραιος.

12.2 Μέση τιμή μιας ΤΜ

Ορισμός 12.6
(Μέση τιμή μιας τυχαίας μεταβλητής) *Αν X είναι μια ΤΜ με ακέραιες τιμές τότε ορίζουμε τη* μέση τιμή *της X μέσω του τύπου*

$$\mathbf{E}X = \sum_{n=-\infty}^{\infty} n f_X(n), \tag{12.5}$$

αν η σειρά συγκλίνει απόλυτα, αν έχουμε δηλαδή

$$\sum_{n=-\infty}^{\infty} |n| f_X(n) < \infty. \tag{12.6}$$

Γενικότερα, αν $X : \Omega \to T \subseteq \mathbb{R}$ είναι οποιαδήποτε διακριτή ΤΜ, με T αριθμήσιμο, τότε η μέση τιμής της ορίζεται από τον τύπο

$$\mathbf{E}X = \sum_{t \in T} t \cdot \mathbf{Pr}\,[X = t], \tag{12.7}$$

και πάλι μόνο όταν

$$\sum_{t \in T} |t| \cdot \mathbf{Pr}\,[X = t] < \infty, \tag{12.8}$$

Παρατήρηση 12.8
Είναι προφανές ότι ο γενικότερος ορισμός (12.7) *συμπίπτει με τον ειδικότερο, για την περίπτωση ακέραιας ΤΜ, ορισμό* (12.5).

Είναι επίσης φανερό ότι αν τα ενδεχόμενα A_s, $s \in S$, με αριθμήσιμο σύνολο δεικτών S, αποτελούν διαμέριση του δειγματικού χώρου Ω και έχουν την ιδιότητα ότι η ΤΜ X είναι σταθερή σε κάθε A_s με τιμή c_s τότε

$$\mathbf{E}X = \sum_{s\in S} c_s \mathbf{Pr}\left[A_s\right].$$

Παρατήρηση 12.9
Αν η ΤΜ X παίρνει πεπερασμένες μόνο τιμές τότε η μέση τιμή της υπάρχει αφού η σειρά (12.5) *δεν είναι παρά ένα πεπερασμένο άθροισμα. Για παράδειγμα, αν X είναι το αποτέλεσμα ενός συνηθισμένου ζαριού, τότε $f_X(n) = \frac{1}{6}\mathbf{1}\left(1 \le n \le 6\right)$ και*

$$\mathbf{E}X = \frac{1}{6}1 + \frac{1}{6}2 + \cdots + \frac{1}{6}6 = 3.5.$$

Γενικότερα, αν η ΤΜ X είναι ομοιόμορφα κατανεμημένη στο $\{0, \ldots, m\}$ τότε $\mathbf{E}X = m/2$.

Παρατήρηση: Η μέση τιμή μιας ΤΜ X, αν υπάρχει, είναι ένας *κυρτός συνδυασμός* των τιμών της X. Κυρτός συνδυασμός κάποιων αριθμών (ή διανυσμάτων) $a_1, a_2, \ldots$ είναι μια ποσότητα της μορφής

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots,$$

όπου $\lambda_j \in [0, 1]$ για κάθε j και

$$\sum_{j=1}^{\infty} \lambda_j = 1.$$

Η διαφορά δηλ. από το συνηθισμένο *γραμμικό συνδυασμό* είναι ο περιορισμός στους συντελεστές ότι πρέπει να είναι μη αρνητικοί και το άθροισμά τους πρέπει να κάνει 1. Αφού λοιπόν $\mathbf{E}X = \sum_{j\in\mathbb{Z}} j\mathbf{Pr}\left[X = j\right]$ και οι συντελεστές μπροστά από τις δυνατές τιμες j της ακέραιας ΤΜ X, δηλ. οι ποσότητες $\mathbf{Pr}\left[X = j\right]$, είναι μη αρνητικοί και έχουν άθροισμα 1, έπεται ότι όντως η μέση τιμή της X είναι κυρτός συνδυασμός των δυνατών τιμών της X (όλων των ακεραίων δηλ.).

✏ **12.15**
Αν $m \le a_j \le M$ για κάθε j και $x = \sum_{j=1}^{\infty} \lambda_j a_j$ είναι ένας κυρτός συνδυασμός των a_j (δηλ. $\forall j\ \lambda_j \in [0, 1]$ και $\sum \lambda_j = 1$) τότε δείξτε ότι

$$m \le x \le M.$$

Συμπεράνετε ότι αν μια ακέραια ΤΜ X ικανοποιεί πάντα $m \le X \le M$ τότε ισχύει και

$$m \le \mathbf{E}X \le M.$$

Γιατί υπάρχει πάντα η μέση τιμή της X υπό αυτές τις υποθέσεις;

Παρατήρηση 12.10
Ο λόγος που απαιτούμε να ισχύει η (12.6) *ή* (12.8) *για να μιλήσουμε για τη σειρά* (12.5) *ή* (12.7) *είναι ότι αν δεν ισχύει η* (12.6) *ή* (12.8) *τότε το άθροισμα της σειράς* (12.5) *ή* (12.7) *εξαρτάται από την οριακή διαδικασία με την οποία το ορίζουμε, ή, με άλλα λόγια, από τη σειρά με την οποία αθροίζουμε τους όρους της* (12.5) *ή της* (12.7).

Αν η ΤΜ X είναι πάντα μη αρνητική και η σειρά (12.6) *ή* (12.8) *αποκλίνουν (ισούνται με $+\infty$), τότε θα θεωρούμε $\mathbf{E}X = \infty$.*

✏ **12.16**
Αν $A \subseteq \Omega$ είναι ένα ενδεχόμενο και $X(\omega) = \mathbf{1}\left(\omega \in A\right)$ υπολογίστε τη $\mathbf{E}X$.

✏ **12.17**
Αν η X ακολουθεί κατανομή Poisson (δείτε (12.4)) με παράμετρο λ δείξτε ότι $\mathbf{E}X = \lambda$.

✏ **12.18**
Δείξτε ότι αν η σταθερά $C > 0$ οριστεί κατάλληλα τότε η συνάρτηση $f(n) = \frac{C}{n^2}\mathbf{1}(n \geq 1)$ είναι πυκνότητα πιθανότητας και ότι οποιαδήποτε ΤΜ με πυκνότητα $f_X \equiv f$ δεν έχει μέση τιμή $\mathbf{E}X$.

✏ **12.19**
Αν η πυκνότητα της X είναι συμμετρική ως πρός το σημείο $x \in \mathbb{R}$, αν δηλ. ισχύει

$$f(n) = f(2x - n), \forall n \in \mathbb{Z},$$

τότε, αν υπάρχει η $\mathbf{E}X$ έχουμε $\mathbf{E}X = x$.

Παράδειγμα 12.15
Αν $T \in \{1, 2, \ldots\}$ είναι ο χρόνος εμφάνισης της πρώτης κορώνας σε μια άπειρη ακολουθία ρίψεως ενός νομίσματος που έρχεται κορώνα με πιθανότητα p, η πυκνότητα της T δίνεται από τον τύπο

$$f_T(n) = p(1-p)^{n-1}\mathbf{1}(n \geq 1),$$

οπότε

$$\mathbf{E}T = \sum_{n=1}^{\infty} p(1-p)^{n-1} n.$$

Παραγωγίζοντας τη σειρά $\sum_{n=0}^{\infty} x^n = (1-x)^{-1}$ κατά όρους παίρνουμε

$$\sum_{n=1}^{\infty} n x^{n-1} = \frac{1}{(1-x)^2}.$$

Εφαρμόζοντας αυτό τον τύπο για $x = 1 - p$ παίρνουμε

$$\mathbf{E}T = p\frac{1}{p^2} = \frac{1}{p}.$$

Ο μέσος χρόνος εμφάνισης δηλ. της πρώτης κορώνας είναι αντιστρόφως ανάλογος της πιθανότητας εμφάνισης κορώνας σε μια ρίψη του νομίσματος.

Η πιο σημαντική ιδιότητα της μέσης τιμής είναι η γραμμικότητά της. Είναι σκόπιμο να τονιστεί εδώ πως, αντίθετα με το Θεώρημα 12.4 παρακάτω, το Θεώρημα 12.2 δεν απαιτεί ανεξαρτησία των ΤΜ. Εκεί έγκειται και η μεγάλη χρησιμότητά του.

Θεώρημα 12.2
Αν οι διακριτές ΤΜ X και Y έχουν μέση τιμή και $\lambda, \mu \in \mathbb{R}$ είναι σταθερές, τότε η ΤΜ $Z = \lambda X + \mu Y$ έχει μέση τιμή και $\mathbf{E}Z = \lambda\mathbf{E}X + \mu\mathbf{E}Y$.

Απόδειξη

Έστω $X : \Omega \to T_1$ και $Y : \Omega \to T_2$, όπου τα σύνολα T_1, T_2 είναι αριθμήσιμα. Ορίζουμε τα ενδεχόμενα

$$A_t = \{X = s\}, \quad (s \in T_1),$$

$$B_t = \{Y = t\} \quad (t \in T_2),$$

και

$$C_{s,t} = \{X = s, Y = t\}, \quad (s \in T_1, t \in T_2).$$

Έχουμε

$$\mathbf{E}X = \sum_{s \in T_1} s\mathbf{Pr}[A_s] = \sum_{s \in T_1} s \sum_{t \in T_2} \mathbf{Pr}[C_{s,t}],$$

και

$$\mathbf{E}Y = \sum_{t\in T_2} s\mathbf{Pr}\left[B_t\right] = \sum_{t\in T_2} t \sum_{s\in T_1} \mathbf{Pr}\left[C_{s,t}\right],$$

οπότε

$$\lambda\mathbf{E}X + \mu\mathbf{E}Y = \sum_{s\in T_1, t\in T_2} \mathbf{Pr}\left[C_{s,t}\right](\lambda s + \mu t) = \mathbf{E}Z,$$

αφού τα ενδεχόμενα $C_{s,t}$, $s \in T_1, t \in T_2$, αποτελούν διαμέριση του Ω στα οποία η ΤΜ Z είναι σταθερή (δείτε Παρατήρηση 12.8).
■

Παράδειγμα 12.16
Στο Παράδειγμα 12.14 μπορούμε να υπολογίσουμε τη $\mathbf{E}X + Y$ χωρίς να χρησιμοποιήσουμε καθόλου τη συνάρτηση πυκνότητας της $X + Y$ που υπολογίσαμε εκεί. Για την X έχουμε από την Άσκηση 12.19 ότι $\mathbf{E}X = m/2$ αφού η ομοιόμορφη κατανομή στο $\{0, \ldots, m\}$ είναι συμμετρική γύρω από το σημείο $m/2$. Τέλος $\mathbf{E}X + Y = \mathbf{E}X + \mathbf{E}Y = 2\mathbf{E}X = 2\frac{m}{2} = m$.

Παράδειγμα 12.17
Έστω ότι η X ακολουθεί τη διωνυμική κατανομή (δείτε Παράδειγμα 12.12) με παραμέτρους p και N, ότι έχουμε δηλαδή

$$f_X(k) = \binom{N}{k} p^k (1-p)N - k\mathbf{1}\left(0 \le k \le N\right).$$

Η X μπορεί να υλοποιηθεί ως το πλήθος των κορωνών σε N ανεξάρτητες ρίψεις ενός νομίσματος που φέρενι κορώνα με πιθανότητα p. Άρα, αν συμβολίσουμε $X_j = \mathbf{1}($ φέρνουμε κορώνα στη j ρίψη$)$ έχουμε

$$X = X_1 + \cdots + X_N,$$

Άρα $\mathbf{E}X = \mathbf{E}X_1 + \cdots + \mathbf{E}X_N = N\mathbf{E}X_1 = Np$.

Παράδειγμα 12.18
Σ' ένα δωμάτιο μπαίνουν N άτομα και αφήνουν τα καπέλα τους στον προθάλαμο, όπου όμως παίζουν κάποια παιδιά και ανακατεύουν τα καπέλα. Φεύγοντας τα N άτομα παίρνουν από ένα καπέλο στην τύχη. Ποιος είναι ο μέσος αριθμός των ατόμων που παίρνουν το δικό τους καπέλο;

Η ΤΜ που μας ενδιαφέρει είναι η X, ο αριθμός των ατόμων, που παίρνουν το δικό τους καπέλο. Ας είναι X_j, $j = 1, \ldots, N$, οι ΤΜ $X_j = \mathbf{1}($ το άτομο j παίρνει το δικό του καπέλο$)$. (Οι ΤΜ X_j δεν είναι ανεξάρτητες. Γιατί;) Είναι φανερό ότι

$$X = X_1 + X_2 + \cdots + X_N.$$

Άρα, από το Θεώρημα 12.2 έχουμε $\mathbf{E}X = \sum_{j=1}^{N} \mathbf{E}X_j$. Επίσης, λόγω της συμμετρίας, έχουμε ότι οι X_j είναι ισόνομες, άρα $\mathbf{E}X = N\mathbf{E}X_1$. Τέλος $\mathbf{E}X_1 = \mathbf{Pr}[$ ο 1 παίρνει το καπέλο του $] = 1/n$, επίσης λόγω της συμμετρίας. Άρα $\mathbf{E}X = 1$. Είναι εντυπωσιακό ότι το $\mathbf{E}X$ δεν εξαρτάται από το N.

Το «σπάσιμο» της ΤΜ X σαν άθροισμα άλλων απλουστέρων, και μάλιστα δεικτριών, ΤΜ είναι ένα πολύ χρήσιμο εργαλείο στη λύση προβλημάτων.

Το παρακάτω είναι εξαιρετικά χρήσιμο σε υπολογισμούς.

Θεώρημα 12.3
Αν X είναι μια διακριτή ΤΜ (όχι αναγκαστικά αριθμητική) και f μια αριθμητική συνάρτηση ορισμένη στο πεδίο τιμών T της X τότε η ΤΜ $f(X)$ έχει μέση τιμή αν

$$\sum_{t\in T} |f(t)|\mathbf{Pr}\left[X = t\right] < \infty,$$

και αυτή τότε ισούται με

$$\mathbf{E}f(X) = \sum_{t\in T} f(t)\mathbf{Pr}\left[X = t\right].$$

Απόδειξη

Η απόδειξη είναι άμεση αν εφαρμόσουμε την Παρατήρηση 12.8 στη διαμέριση $\Omega = \bigcup_{t\in T}\{X = t\}$.
■

Παρατήρηση 12.11
Μετά το Θεώρημα 12.3 είναι φανερό πως η συνθήκες (12.6) και (12.8) δεν είναι τίποτε άλλο από τη συνθήκη $\mathbf{E}|X| < \infty$ (η μέση τιμή μιας μη αρνητικής ΤΜ υπάρχει πάντα και είναι πεπερασμένος αριθμός ή $+\infty$).

✏ **12.20**
Όταν αγοράζετε ένα συγκεκριμένο προϊόν υπάρχει πάντα μέσα στη συσκευασία ένα παιχνίδι-έκπληξη. Υπάρχουν c διαφορετικά τέτοια παιχνίδια που μπορεί να βρείτε μέσα στη συσκευασία και όλα αυτά τα παιχνίδια είναι εξίσου πιθανό να εμφανιστούν. Αγοράζετε ένα τέτοιο προϊόν κάθε μέρα. Ποιος είναι ο μέσος αριθμός ημερών που περνάει από τότε που θα βρείτε το j-οστό νέο παιχνίδι μέχρι να βρείτε το $(j+1)$-οστό νέο παιχνίδι; Ποιος είναι ο μέσος αριθμός ημερών που περνάει έως ότου βρείτε και τα c διαφορετικά παιχνίδια;

Θεώρημα 12.4
Αν οι ΤΜ X και Y είναι ανεξάρτητες και έχουν μέσες τιμές τότε και η XY έχει μέση τιμή και $\mathbf{E}XY = \mathbf{E}X\mathbf{E}Y$.

Απόδειξη

Έστω $X : \Omega \to T_1$ και $Y : \Omega \to T_2$, όπου τα σύνολα T_1, T_2 είναι αριθμήσιμα. Όπως και στην απόδειξη του Θεωρήματος 12.2 ορίζουμε τα ενδεχόμενα

$$C_{s,t} = \{X = s, Y = t\}, \quad (s \in T_1, t \in T_2).$$

Έχουμε

$$\begin{aligned}
\mathbf{E}|XY| &= \sum_{s\in T_1, t\in T_2} |st|\mathbf{Pr}\left[C_{s,t}\right] \\
&= \sum_{s\in T_1, t\in T_2} |st|\mathbf{Pr}\left[X = s\right]\mathbf{Pr}\left[Y = t\right] \quad \dagger \\
&= \sum_{s\in T_1} |s|\mathbf{Pr}\left[X = s\right] \cdot \sum_{t\in T_2} |t|\mathbf{Pr}\left[Y = t\right] \\
&= \mathbf{E}|X|\mathbf{E}|Y| < \infty
\end{aligned}$$

(†: από ανεξαρτησία των X, Y), οπότε έχουμε δείξει ότι η XY έχει μέση τιμή. Ομοίως

$$\begin{aligned}
\mathbf{E}XY &= \sum_{s\in T_1, t\in T_2} st\mathbf{Pr}\left[C_{s,t}\right] \\
&= \sum_{s\in T_1, t\in T_2} st\mathbf{Pr}\left[X = s\right]\mathbf{Pr}\left[Y = t\right] \quad \ddagger \\
&= \sum_{s\in T_1} s\mathbf{Pr}\left[X = s\right] \cdot \sum_{t\in T_2} t\mathbf{Pr}\left[Y = t\right] \\
&= \mathbf{E}X\mathbf{E}Y
\end{aligned}$$

(‡: από ανεξαρτησία των X, Y).
■

Παρατήρηση 12.12
Ομοίως προκύπτει ότι αν οι $X_1, \ldots, X_N$ είναι ένα ανεξάρτητο σύνολο από ΤΜ τότε $\mathbf{E}X_1 \cdots X_N = \mathbf{E}X_1 \cdots \mathbf{E}X_N$.

Παρατήρηση 12.13
Η συνθήκη «X, Y ανεξάρτητες» δε μπορεί να παραλειφθεί στο Θεώρημα 12.4. Ας είναι, για παράδειγμα, A και B δύο ξένα μεταξύ τους ενδεχόμενα με θετική πιθανότητα το καθένα, και $X = \mathbf{1}_A$, $Y = \mathbf{1}_B$ οι αντίστοιχες δείκτριες ΤΜ (δείτε το Παράδειγμα 12.8). Έχουμε τότε $XY = \mathbf{1}_{A\cap B} = \mathbf{1}_\emptyset$ άρα $\mathbf{E}XY = 0$ ενώ $\mathbf{E}X = \mathbf{Pr}[A] > 0$ και $\mathbf{E}Y = \mathbf{Pr}[B] > 0$.

Παράδειγμα 12.19
Ένα σωμάτιο εκτελεί ένα «τυχαίο περίπατο» ως εξής: τη χρονική στιγμή 0 βρίσκεται στη θέση 0 του άξονα των ακεραίων αριθμών. Σε κάθε ακέραια χρονική στιγμή ρίχνει ένα τίμιο νόμισμα και αν έρθει κορώνα μετακινείται μια μονάδα αριστερά, αλλιώς πάει μια μονάδα δεξιά. Αν λοιπόν γράψουμε X_j για τη μετακίνηση του σωματίου κατά τη χρονική στιγμή j έχουμε $X_j \in \{-1, +1\}$ και $\mathbf{Pr}[X_j = -1] = \mathbf{Pr}[X_j = +1] = 1/2$, άρα $\mathbf{E}X_j = \frac{1}{2}(-1) + \frac{1}{2}1 = 0$. Η θέση του σωματιδίου τη χρονική στιγμή n, έστω S_n, μπορεί να γραφεί ως

$$S_n = X_1 + \cdots + X_n,$$

οπότε, από τη γραμμικότητα της μέσης τιμής έχουμε επίσης $\mathbf{E}S_n = 0$ για κάθε n.

Ας υπολογίσουμε τέλος τη «μέση τετραγωνική απόσταση» του σωματιδίου από το 0 τη χρονική στιγμή n. Αυτή είναι η ποσότητα $\sqrt{\mathbf{E}S_n^2}$ και έχουμε

$$S_n^2 = (X_1 + \cdots + X_n)^2 = \sum_{j=1}^{n} X_j^2 + 2\sum_{i<j} X_i X_j,$$

όπου το δεύτερο άθροισμα είναι για όλους τους δείκτες $i, j = 1, \ldots, n$, με $i < j$. Επειδή X_i και X_j είναι ανεξάρτητες αν $i \neq j$ και $\mathbf{E}X_i = 0$ έχουμε ότι οι μέσες τιμές όλων των προσθετέων στο δεύτερο άθροισμα είναι 0. Τέλος έχουμε $\mathbf{E}X_j^2 = 1$ αφού $X_j^2 = 1$ πάντα. Άρα $\mathbf{E}S_n^2 = n$ και η μέση τετραγωνική απόσταση από το 0 είναι $\sqrt{n}$.

✏ **12.21**
Έχουμε n παίκτες που ρίχνουν από ένα ζάρι ο καθένας. Αν X είναι το πλήθος των ζευγών που φέρνουν τον ίδιο αριθμό να βρεθεί η $\mathbf{E}X$.

✏ **12.22**
Έχουμε n ζευγάρια και από αυτά τα $2n$ άτομα ένα τυχαίο υποσύνολο μεγέθους m πεθαίνει. Να βρεθεί ο μέσος αριθμών των ζευγαριών που έχουν απομείνει.

✏ **12.23**
Έχουμε δύο κουτιά που στην αρχή περιέχουν n κόκκινους βώλους το πρώτο και n μπλε βώλους το δεύτερο. Σε κάθε χρονική στιγμή βάζουμε από ένα χέρι σε κάθε κουτί, πιάνουμε από ένα βώλο και τους εναλλάσσουμε. Να βρεθεί ο μέσος αριθμός κόκκινων βώλων στο πρώτο κουτί μετά από k τέτοιες εναλλαγές.
💡 *Ένας κόκκινος βώλος είναι στο πρώτο κουτί μετά από k βήματα αν και μόνο αν έχει επιλεγεί για εναλλαγή ένα άρτιο αριθμό φορών.*

✏ **12.24**
Η ακέραια ΤΜ X έχει πυκνότητα $f_X(n)$. Εκτελούμε το πείραμα που δίνει τιμή στη X αλλά δε βλέπουμε την τιμή αυτή. Πρέπει να τη μαντέψουμε. Αν η τιμή που θα πούμε, έστω ο ακέραιος t, είναι μικρότερη από τη X τότε πληρώνουμε $b \cdot y$ ευρώ, όπου $y = |X - t|$. Αν είναι μεγαλύτερη τότε πληρώνουμε $a \cdot y$. Οι αριθμοί a, b όπως και η συνάρτηση $f_X(n)$ μας είναι γνωστοί. Πώς πρέπει να επιλέξουμε το t ώστε να έχουμε το μικρότερο δυνατό μέσο *κόστος;*

Σχήμα 12.3: Ο Paul Erdős.

✏ **12.25**

Ο Paul Erds (ουγγρικά: Erdős Pál) υπήρξε από τους πρωτεργάτες και ο κυριότερος προπαγανδιστής της λεγόμενης «<πιθανοθεωρητικής μεθόδου» (probabilistic method) στα μαθηματικά και ιδιαίτερα σε αυτό που σήμερα ονομάζεται «διακριτά μαθηματικά» (θεωρία αριθμών, συνδυαστική, θεωρητική επιστήμη υπολογιστών). Η πρωσοποποίηση της ιδιορρυθμίας, ο Erds έζησε μια ζωή γεμάτη μαθηματικά και μόνο, τα οποία σημάδεψε με δεκάδες σημαντικά αποτελέσματα και εκατοντάδες συνεργασίες σε όλο τον κόσμο.

Χαρακτηριστικό μιας πιθανοθεωρητικής απόδειξης (ειδική περίπτωση μιας υπαρξιακής απόδειξης) είναι ότι δείχνουμε την ύπαρξη ενός αντικειμένου με κάποιες επιθυμητές ιδιότητες χωρίς να «κατασκευάσουμε» ένα τέτοιο αντικείμενο, τουλάχιστον όχι με την κλασική έννοια του όρου κατασκευή. Αντίθετα δείχνουμε ότι ένα κατάλληλο στατιστικό πείραμα έχει θετική (και συνήθως μεγάλη) πιθανότητα να παραγάγει ένα τέτοιο αντικείμενο.

Υποθέστε ότι έχετε ένα πλήρες γράφημα με n κορυφές (n σημεία δηλ. που όλα ενώνονται με όλα τα άλλα, με πλήθος ακμών $\binom{n}{2}$) και ότι κάθε ακμή του μπορεί να βαφεί κόκκινη ή μπλε. Δείξτε ότι μπορείτε να επιλέξετε τα χρώματα των ακμών έτσι ώστε το πλήθος των μονοχρωματικών τριγώνων που σχηματίζονται να είναι το πολύ $\frac{1}{4}\binom{n}{3}$.

Σχήμα 12.4: Για την Άσκηση 12.26.

✏ **12.26**

Έχουμε 1000 κουτιά στη σειρά (στις θέσεις 1, 2, 3, ..., 1000).

Δείξτε ότι μπορούμε να τα βάψουμε με δύο χρώματα, π.χ. κόκκινα ή μπλε, με τέτοιο τρόπο ώστε να μην υπάρχει αριθμητική πρόοδος μήκους 20 από κουτιά που να είναι όλα το ίδιο χρώμα. (Δείτε το Σχήμα 12.4.)

12.3 Διασπορά μιας ΤΜ και ανισότητες απόκλισης

Ορισμός 12.7

(Διασπορά μιας τυχαίας μεταβλητής) *Αν X είναι μια ΤΜ με μέση τιμή $\mu = \mathbf{E}X$ τότε η* διασπορά *της X είναι η ποσότητα $\mathbb{V}ar[X] = \sigma^2(X) = \mathbf{E}(X-\mu)^2$. Ορίζουμε επίσης την* τυπική απόκλιση *της X ως την ποσότητα $\sigma(X) = \sqrt{\mathbb{V}ar[X]}$.*

Παρατήρηση 12.14
Από τον Ορισμό 12.7 γίνεται φανερό ότι η διασπορά και η τυπική απόκλιση μιας ΤΜ μετρούν το πόσο πιθανό είναι να αποκλίνει η ΤΜ X από τη μέση τιμή της.

Παρατήρηση 12.15
Επειδή η ΤΜ $(X-\mu)^2 \geq 0$ η διασπορά της X υπάρχει πάντα και είναι πεπερασμένος μη αρνητικός αριθμός ή $+\infty$, υπό την προϋπόθεση μόνο ότι η X έχει μέση τιμή, δηλ. $\mathbf{E}|X| < \infty$.

✏ **12.27**
Αν η ΤΜ έχει $\mathbf{E}X^2 < \infty$ τότε έχουμε αναγκαστικά και $\mathbf{E}|X| < \infty$.
Γράψτε $X = Y + Z$, όπου $Y = X \cdot \mathbf{1}(|X| \leq 1)$ και $Z = X - Y$. Δείξτε ότι $\mathbf{E}|Y| < \infty$ και $\mathbf{E}|Z| < \infty$.

✏ **12.28**
Αν $\mathbf{E}X^2 < \infty$ τότε ισχύει $\mathbb{V}ar[X] = \mathbf{E}X^2 - \mathbf{E}X^2$.

✏ **12.29**
Δείξτε ότι αν c είναι σταθερά τότε $\mathbb{V}ar[X-c] = \mathbb{V}ar[X] = \mathbb{V}ar[-X]$.

✏ **12.30**
Δείξτε ότι αν $\mathbb{V}ar[X] = 0$ τότε $X = \mathbf{E}X$ σχεδόν σίγουρα.

Παράδειγμα 12.20
Αν η X είναι ομοιόμορφα κατανεμημένη στο $\{0, \ldots, m\}$ τότε

$$\mathbf{E}X^2 = \sum_{k=0}^{m} \frac{1}{m+1} k^2 = \frac{1}{6} m(2m+1)$$

χρησιμοποιώντας το αποτέλεσμα του Προβλήματος 1.14. Επίσης $\mathbf{E}X = m/2$ αφού η πυκνότητα της X είναι συμμετρική γύρω από το $m/2$. Οπότε, χρησιμοποιώντας τον τύπο του Προβλήματος 12.28 έχουμε

$$\mathbb{V}ar[X] = \frac{1}{6} m(2m+1) - \frac{m^2}{4} = \frac{m(m+2)}{12}.$$

Θεώρημα 12.5
Αν οι ΤΜ $X_1, \ldots, X_n$ είναι ανεξάρτητες ανά δύο *και έχουν μέση τιμή τότε*

$$\mathbb{V}ar[X_1 + \cdots + X_n] = \mathbb{V}ar[X_1] + \cdots + \mathbb{V}ar[X_n].$$

Απόδειξη

Ας είναι $\mu_j = \mathbf{E}X_j$, $j = 1, \ldots, n$. Η μέση τιμή της $S = X_1 + \cdots + X_n$ υπάρχει και ισούται με $\mu = \mu_1 + \cdots + \mu_n$, οπότε

$$\begin{aligned}
\mathbb{V}ar[S] &= \mathbf{E}(S-\mu)^2 \\
&= \mathbf{E}\left(\sum_{j=1}^{n}(X_j - \mu_j)\right)^2 \\
&= \mathbf{E}\sum_{j=1}^{n}(X_j-\mu_j)^2 + 2\sum_{i<j}(X_i-\mu_i)(X_j-\mu_j) \\
&= \sum_{j=1}^{n}\mathbb{V}ar[X_j] + 2\sum_{i<j}\mathbf{E}(X_i-\mu_i)(X_j-\mu_j).
\end{aligned}$$

Η απόδειξη τελειώνει με την παρατήρηση ότι $\mathbf{E}(X_i - \mu_i)(X_j - \mu_j) = 0$ αν $i \neq j$, αφού οι ΤΜ $X_i - \mu_i$ και $X_j - \mu_j$ είναι ανεξάρτητες και έχουν μέση τιμή 0.
■

Παράδειγμα 12.21
Έστω ότι η X ακολουθεί τη διωνυμική κατανομή (δείτε Παράδειγμα 12.12) με παραμέτρους p και N. Η X μπορεί να υλοποιηθεί ως το πλήθος των κορωνών σε N ανεξάρτητες ρίψεις ενός νομίσματος που φέρνει κορώνα με πιθανότητα p. Άρα, αν συμβολίσουμε $X_j = \mathbf{1}(i$ φέρνουμε κορώνα στη j ρίψη$)$ έχουμε

$$X = X_1 + \cdots + X_N,$$

Άρα $\mathbb{V}ar[X] = \mathbb{V}ar[X_1] + \cdots + \mathbb{V}ar[X_N] = N\mathbb{V}ar[X_1] = Np(1-p)$, αφού εύκολα βλέπουμε ότι $\mathbb{V}ar[X_1] = p(1-p)$.

Θεώρημα 12.6
(Ανισότητα Markov) *Αν $X \geq 0$ έχει μέση τιμή $\mu \in \mathbb{R}$ τότε*

$$\mathbf{Pr}[X \geq \lambda\mu] \leq \frac{1}{\lambda}.$$

Απόδειξη

Ορίζουμε το ενδεχόμενο $A = \{X \geq \lambda\mu\}$. Αν T είναι το σύνολο τιμών της X τότε, από τον ορισμό της $\mathbf{E}X$, έχουμε

$$\begin{aligned}
\mu &= \sum_{t\in T} t\mathbf{Pr}[X = t] \\
&= \sum_{t\in T, t<\lambda\mu} t\mathbf{Pr}[X = t] + \sum_{t\in T, t\geq\lambda\mu} t\mathbf{Pr}[X = t] \\
&\geq \sum_{t\in T, t\geq\lambda\mu} t\mathbf{Pr}[X = t] \\
&\geq \sum_{t\in T, t\geq\lambda\mu} \lambda\mu\mathbf{Pr}[X = t] \\
&= \lambda\mu\mathbf{Pr}[A].
\end{aligned}$$

Η ανισότητα προκύπτει αφού διαρέσουμε δια του $\lambda\mu$.
■

Πόρισμα 12.1
(Ανισότητα Chebyshev) *Αν η X έχει πεπερασμένη διασπορά σ^2 και μέση τιμή μ τότε*

$$\mathbf{Pr}[|X - \mu| \geq \lambda\sigma] \leq \frac{1}{\lambda^2}.$$

Απόδειξη

Ορίζουμε τη μη-αρνητική ΤΜ $Y = (X - \mu)^2$ με $\mathbf{E}Y = \sigma^2$ και εφαρμόζουμε σε αυτή την ανισότητα του Markov (Θεώρημα 12.6). Παίρνουμε

$$\mathbf{Pr}[|X - \mu| \geq \lambda\sigma] = \mathbf{Pr}\left[Y \geq \lambda^2\sigma^2\right] \leq \frac{1}{\lambda^2}.$$

■

✏ **12.31**
(Γενικευμένη ανισότητα Chebyshev) *Έστω $g : [0, \infty) \to [0, \infty)$ μια αυστηρά αύξουσα συνάρτηση και X μια ΤΜ τέτοια ώστε $\mathbf{E}g(|X|) < \infty$. Δείξτε ότι*

$$\mathbf{Pr}\left[|X| \geq \lambda\right] \leq \frac{\mathbf{E}g(|X|)}{g(\lambda)}.$$

✏ **12.32**
(Ακολουθούμε το συμβολισμό και ορολογία του Παραδείγματος 12.19.) Χρησιμοποιήστε την ανισότητα του Chebyshev για να βρείτε ένα άνω φράγμα για την $\mathbf{Pr}\left[|S_n| > n/10\right]$.

✏ **12.33**
Έστω X μια ΤΜ που ακολουθεί τη γεωμετρική κατανομή (12.2) με παράμετρο $p = 1/2$. Βρείτε άνω φράγματα για την ποσότητα $\mathbf{Pr}\left[X \geq 10\right]$ χρησιμοποιώντας την ανισότητα Markov και την ανισότητα του Chebyshev και συγκρίνετέ τα μεταξύ τους καθώς και με την ακριβή τιμή γι' αυτή την ποσότητα.

✏ **12.34**
Ας υποθέσουμε ότι έχουμε ένα μεγάλο πληθυσμό ανθρώπων του οποίου θέλουμε να εκτιμήσουμε το μέσο ύψος αλλά και το πόσο αυτό κυμαίνεται μέσα στον πληθυσμό. Λίγο πιο αυστηρά, θέλουμε να εκτιμήσουμε τη μέση τιμή $\mathbf{E}X$ και τη διασπορά $\sigma^2(X)$ της τυχαίας μεταβλητής X που προκύπτει αν επιλέξουμε ένα τυχαίο άτομο και μετρήσουμε το ύψος του, με όλα τα άτομα εξίσου πιθανά να επιλεγούν.

Ο τρόπος που το κάνουμε είναι να διαλέξουμε N φορές τυχαία (N μεγάλο) ένα άτομο και να μετρήσουμε το ύψος του, έστω $x_i, i = 1, \ldots, N$. Έπειτα εκτιμούμε το μέσο ύψος του πληθυσμού από την ποσότητα

$$\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i.$$

Θυμόμαστε τώρα το γενικό ορισμό $\sigma^2(X) = \mathbf{E}(X - \mathbf{E}X)^2$ και εκτιμούμε ανάλογα τη διασπορά του ύψους από την ποσότητα

$$S^2 = \frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2.$$

Όμως ο στατιστικός φίλος μας, στον οποίο δείχνουμε τη μέθοδό μας, ισχυρίζεται ότι δεν πρέπει να το κάνουμε έτσι αλλά ως εξής:

$$S^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \overline{x})^2.$$

Η αλήθεια είναι ότι αυτές οι δύο ποσότητες ελάχιστα διαφέρουν μεταξύ τους όταν το N είναι μεγάλο. Όμως ποιος έχει δίκιο;

12.4 Γεννήτριες συναρτήσεις

Ορισμός 12.8
(Γεννήτρια συνάρτηση) *Αν X είναι μια ΤΜ που παίρνει τιμές στο σύνολο $\mathbb{N} = \{0, 1, 2, \ldots\}$ τότε η* γεννήτρια συνάρτηση *της X είναι η συνάρτηση*

$$\Phi_X(t) = \mathbf{E}t^X = \sum_{n=0}^{\infty} f_X(n)t^n, \quad (|t| \leq 1).$$

Παρατήρηση 12.16
Αποδεικνύεται ότι η άπειρη σειρά στον ορισμό 12.8 συγκλίνει για όλα τα t με $|t| \leq 1$.

Παράδειγμα 12.22
Αν $X = c$ σχεδόν σίγουρα τότε $\Phi_X(t) = t^c$.

Παράδειγμα 12.23
Αν η X ακολουθεί γεωμετρική κατανομή (12.2) με παράμετρο p τότε

$$\begin{aligned}\Phi_X(t) &= \sum_{n=1}^{\infty} t^n p(1-p)^{n-1} \\ &= \frac{p}{1-p}\sum_{n=1}^{\infty}(t(1-p))^n \\ &= \frac{p}{1-p}\left(\frac{1}{1-t(1-p)}-1\right) \\ &= \frac{pt}{1-(1-p)t}.\end{aligned}$$

Παράδειγμα 12.24
Αν η X ακολουθεί τη διωνυμική κατανομή (12.3) με παραμέτρους N και p, τότε

$$\begin{aligned}\Phi_X(t) &= \sum_{n=0}^{N} t^n \binom{N}{n} p^n (1-p)^{N-n} \\ &= \sum_{n=0}^{N} \binom{N}{n} (tp)^n (1-p)^{N-n} \\ &= (1-p+pt)^N,\end{aligned}$$

(με εφαρμογή του διωνυμικού Θεωρήματος 4.4.

Παράδειγμα 12.25
Αν η X ακολουθεί κατανομή Poisson (12.4) με παράμετρο $\lambda > 0$ τότε

$$\Phi_X(t) = \sum_{n=0}^{\infty} t^n e^{-\lambda}\frac{\lambda^n}{n!} == e^{-\lambda}\sum_{n=0}^{\infty}\frac{(t\lambda)^n}{n!} = e^{-\lambda}e^{t\lambda} = e^{\lambda(1-t)}.$$

Θεώρημα 12.7
Αν $X_1, \ldots, X_r$ είναι ανεξάρτητες ΤΜ και $Y = X_1 + \cdots + X_r$ τότε

$$\Phi_Y(t) = \Phi_{X_1}(t)\cdots\Phi_{X_r}(t).$$

Απόδειξη

$\Phi_Y(t) = \mathbf{E}t^Y = \mathbf{E}t^{X_1}\cdot t^{X_2}\cdots t^{X_r}$. Οι ΤΜ $t^{X_1}, \ldots, t^{X_r}$ είναι κι αυτές ανεξάρτητες άρα $\Phi_Y(t) = \mathbf{E}t^{X_1}\cdots\mathbf{E}t^{X_r} = \Phi_{X_1}(t)\cdots\Phi_{X_r}(t)$.
■

Το επόμενο πολύ σημαντικό θεώρημα το δεχόμαστε χωρίς απόδειξη.

Θεώρημα 12.8
(Θεώρημα Μοναδικότητας της Γεννήτριας Συνάρτησης) *Αν δύο ΤΜ X και Y (που παίρνουν τιμές στο $\mathbb{N}$) έχουν την ίδια γεννήτρια συνάρτηση τότε είναι ισόνομες.*

Χρησιμοποιώντας τα Θεωρήματα 12.7 και 12.8 μπορούμε εύκολα να δείξουμε το ακόλουθο.

Θεώρημα 12.9
(α) Αν οι $X_1, \ldots, X_r$ είναι ανεξάρτητες και η X_i ακολουθεί τη διωνυμική κατανομή με παραμέτρους N_i και p τότε η $Y = X_1 + \cdots + X_r$ ακολουθεί τη διωνυμική κατανομή με παραμέτρους $N_1 + \cdots + N_r$ και p.
(β) Αν οι $X_1, \ldots, X_r$ είναι ανεξάρτητες και η X_i ακολουθεί τη κατανομή Poisson με παράμετρο $\lambda_i > 0$ τότε η $Y = X_1 + \cdots + X_r$ ακολουθεί τη κατανομή Poisson με παράμετρο $\lambda_1 + \cdots + \lambda_r$.

Απόδειξη

(α) Έχουμε $\Phi_{X_i}(t) = (1 - p + pt)^{N_i}$ και από την ανεξαρτησία έχουμε

$$\Phi_Y(t) = \Phi_{X_1}(t) \cdots \Phi_{X_r}(t) = (1 - p + pt)^{N_1 + \cdots + N_r}.$$

Αλλά και η διωνυμική κατανομή με παραμέτρους $N_1 + \cdots + N_r$ και p έχει την ίδια γεννήτρια συνάρτηση, άρα (Θεώρημα 12.8) αυτή είναι η κατανομή της Y.

(β) Έχουμε $\Phi_{X_i}(t) = e^{\lambda_i(1-t)}$ και από την ανεξαρτησία έχουμε

$$\Phi_Y(t) = \Phi_{X_1}(t) \cdots \Phi_{X_r}(t) = e^{(\lambda_1 + \cdots + \lambda_r)(1-t)}.$$

Αλλά και η κατανομή Poisson με παράμετρο $\lambda_1 + \cdots + \lambda_r$ έχει την ίδια γεννήτρια συνάρτηση, άρα (Θεώρημα 12.8) αυτή είναι η κατανομή της Y.
■

✏ **12.35**
Υπολογίστε τη γεννήτρια συνάρτηση της ομοιόμορφης κατανομής στο $\{a, \ldots, b\}$, $0 \leq a < b$.

✏ **12.36**
Αν η ΤΜ X έχει γεννήτρια συνάρτηση τη $\Phi_X(t)$ ποια είναι η πυκνότητα μιας ΤΜ που έχει γεννήτρια συνάρτηση τη $\Phi_X(t^2)$;

12.5 Video Κεφαλαίου

12.1
Η έννοια της τυχαίας μεταβλητής (ΤΜ). (video και συνοδευτικές ερωτήσεις, 9:35 λεπτά).

12.2
Παράδειγμα ΤΜ. Πυκνότητα πιθανότητας. (video και συνοδευτικές ερωτήσεις, 12:51 λεπτά).

12.3
Συναρτήσεις πυκνότητας και κατανομής μιας ΤΜ. (video και συνοδευτικές ερωτήσεις, 16:35 λεπτά).

12.4
Γεωμετρική και Διωνυμική κατανομή. (video και συνοδευτικές ερωτήσεις, 19:37 λεπτά).

12.5
Μέση τιμή μιας ΤΜ. (video και συνοδευτικές ερωτήσεις, 13:02 λεπτά).

12.6
Γραμμικότητα της μέσης τιμής και εφαρμογές. (video και συνοδευτικές ερωτήσεις, 24:51 λεπτά).

12.7
n καπέλα στον αέρα. (video και συνοδευτικές ερωτήσεις, 4:52 λεπτά).

12.8
m μπάλες σε n κουτιά. *(video και συνοδευτικές ερωτήσεις, 8:04 λεπτά)*.

12.9
Το πρόβλημα της συλλογής κουπονιών. *(video και συνοδευτικές ερωτήσεις, 17:35 λεπτά)*.

12.10
Χρονιές με ρεκόρ βροχόπτωσης. *(video και συνοδευτικές ερωτήσεις, 10:22 λεπτά)*.

12.11
Ενδεχόμενα που εξαρτώνται από μια ΤΜ. Ανεξαρτησία ΤΜ. *(video και συνοδευτικές ερωτήσεις, 14:15 λεπτά)*.

12.12
Κοινή κατανομή ΤΜ. Μέση τιμή του γινομένου ανεξαρτήτων ΤΜ. *(video και συνοδευτικές ερωτήσεις, 12:07 λεπτά)*.

12.13
Διασπορά μιας ΤΜ. *(video και συνοδευτικές ερωτήσεις, 13:36 λεπτά)*.

12.14
Διασπορά αθροίσματος ανεξαρτήτων ΤΜ. *(video και συνοδευτικές ερωτήσεις, 14:29 λεπτά)*.

12.15
Μέση τιμή και διασπορά γεωμετρικής κατανομής. *(video και συνοδευτικές ερωτήσεις, 13:27 λεπτά)*.

12.16
Η μέση τιμή και διασπορά της κατανομής Poisson(λ). *(video και συνοδευτικές ερωτήσεις, 8:57 λεπτά)*.

12.17
Η μέση τιμή και διασπορά του τυχαίου περίπατου. *(video και συνοδευτικές ερωτήσεις, 7:57 λεπτά)*.

12.18
3η και 4η ροπή του τυχαίου περίπατου. *(video και συνοδευτικές ερωτήσεις, 20:03 λεπτά)*.

12.19
Η ανισότητα του Markov. *(video και συνοδευτικές ερωτήσεις, 17:51 λεπτά)*.

12.20
Γενικευμένη ανισότητα Markov. Ανισότητα Chebyshev. *(video και συνοδευτικές ερωτήσεις, 20:38 λεπτά)*.

12.21
Συνδιακύμανση δύο ΤΜ. *(video και συνοδευτικές ερωτήσεις, 4:40 λεπτά)*.

12.22
Ανισότητα Cauchy-Schwarz. Συντελεστής συσχέτισης δύο ΤΜ. *(video και συνοδευτικές ερωτήσεις, 31:38 λεπτά)*.

12.23
Κοινή πυκνότητα δύο ΤΜ. Περιθώριες πυκνότητες. *(video και συνοδευτικές ερωτήσεις, 16:16 λεπτά)*.

12.24
Οι περιθώριες δεν καθορίζουν την κοινή πυκνότητα. (video και συνοδευτικές ερωτήσεις, 8:59 λεπτά).

12.25
Κοινή πυκνότητα δύο ανεξαρτήτων ΤΜ. (video και συνοδευτικές ερωτήσεις, 17:49 λεπτά).

12.26
Δέσμευση ΤΜ ως προς ενδεχόμενο. (video και συνοδευτικές ερωτήσεις, 17:14 λεπτά).

12.27
Δεσμευμένη μέση τιμή μιας ΤΜ. (video και συνοδευτικές ερωτήσεις, 40:22 λεπτά).

12.28
Μέση τιμή αθροίσματος τυχαίου πλήθους ΤΜ. (video και συνοδευτικές ερωτήσεις, 12:53 λεπτά).

12.29
Δεσμευμένη διασπορά. (video και συνοδευτικές ερωτήσεις, 23:16 λεπτά).

Βιβλιογραφία Κεφαλαίου

[1] Charles Miller Grinstead and James Laurie Snell. *Introduction to probability*. American Mathematical Soc., 2012.

[2] Paul Gerhard Hoel, Sidney C Port, and Charles J Stone. *Introduction to probability theory*. Vol. 12. Houghton Mifflin Boston, 1971.

[3] Sheldon Ross. *A first course in probability*. Macmillan, New York, NY, 1976.

Ευρετήριο